Tableau de matières

Liste des figures 8
Liste des tableaux ……..9
Abréviations 10
Introduction 11

Chapitre I: Principe de Data Loss Prevention……....12

1. **Organisme D'accueil** ……12
2. **Constats, Risques & Enjeux** ……13
3. **Qu'est-ce que le DLP ?** …….…14
4. **Sources des violations de données** ……...15
5. **Fonctionnement de DLP** ……....16
6. **les avantages principaux du DLP** …….. ……..…18
7. **Conclusion** ……..…...19

Chapitre II : Etude et présentation des différents acteurs du marché ….……20

1. CA DLP (Orchestria) ……..…..20
2. EMC/RSA ……....21
3. Symantec DLP ……..23
4. Vericept ……24
5. Websense ……...25
6. McAfee Data Loss Prevention ……..……26

2. **Conclusion** ……....29

Chapitre III : Etude comparative…….……30
1. **Le Choix de la solution** ……...31
2. **Etude comparative** ……31
   2.1 Etude FORRESTER ……...……31
   2.2 Etude Gartner ……..……...…34
3. **Conclusion** ……. ……36

Chapitre VI : Focus sur McAfee Host Data Loss Prevention ……...……..……..37

1. **Qu'est-ce que McAfee Host Data Loss Prevention ?**.....37
2. **Présentation des composants et interactions** …….....37
3. **Fonctionnement de McAfee Data Loss Prevention**……..39
4. **Chiffrement** …….…41
5. **Console du gestionnaire de stratégies Host DLP** …….…42
6. **Quelle Démarche Adopter ?** …….…43
7. **Conclusion** ……...43

Chapitre V : La réalisation de la maquette de test ……..……...44

1. **Architecture de la maquette ……...44**
2. **Installation et configuration de HDLP ……..44**
3. **Classification de contenu sensible ……...59**
4. **Règle de protection ……...62**
5. **Rôle du moniteur Host DLP ……72**
6. **Administration de la base de données et génération de rapport……...73**
7. **Conclusion…….…73**

Conclusion ……...…75

Annexe ……76

Bibliographiques ……....78

- **Liste de figures**

Figure1 : Nombres de violations par an : Source Verizon 2009 Data Breach Investigations Repor

Figure 2 : Les causes communes de brèches de sécurité interne D'après "Deloitte'sGlobal Security Survey"

Figure 3 : Plateforme CA DLP
Figure 4 : Plateforme RSA® DLP
Figure 5 : Plateforme Symantec DLP
Figure 6 : Architecture de Vericept DLP
Figure 7 : Plateforme de McAfee DLP
Figure 8 : The_Forrester_Wave_DataLeakPrevention_Q2_2008
Figure 9 : suite de The_Forrester_Wave_DataLeakPrevention_Q2_2008
Figure 10 : Magic Quadrant for Content-Aware Data Loss Prevention
Figure 11 : McAfee Host Data Loss Prevention
Figure 12 : Flux de travail McAfee Host Data Loss Prevention
Figure 13 : Gestionnaire de stratégies Host DLP dans la console ePolicy Orchestrator 4.5
Figure 14 : Page de test du service WCF DLP
Figure 15 : Règles et actions associées

- **Liste d tableaux**

Tableau 1 : Matériels requise pour installation de HDLP
Tableau 2 : Les systèmes d'exploitation pris en charge pour installation de HDLP
Tableau 3 : Logiciel nécessaire sur le serveur pour installation de HDLP

Abreviations

- **DLP** : data loss prevention
- **EMC Document** : Content Storage Services permet aux utilisateurs de définir et d'exécuter les politiques de stockage de contenu.
- **EPO** : ePolicy Orchestrator
- **FBI** : Federal Bureau of Investigation
- **Forrester** : une société de recherche indépendante qui fournit des conseils pragmatiques aux chefs mondiaux en gestion des affaires et de la technologie
- **FTP :** File transfer protocol
- **Gartner** : une entreprise américaine de conseil et de recherche.
- **HIPAA** : Health Insurance Portability and Accountability Act
- **HTTP/HTTPS** : HyperText Transfer Protocol /sécurisé
- **ICAP** : Internet Content Adaptation Protocol
- **IIS** : Internet Information Services, communément appelé IIS, est le logiciel de serveur services Web (ou FTP, SMTP, HTTP etc.) de la plateforme Windows NT.
- **IM** : messagerie instantanée
- **IPod** : un baladeur numérique d'Apple
- **Microsoft SharePoint** : Solution de portail collaboratif de Microsoft permettant l'administration de la gestion électronique des documents.
- **MTA** : agent de transfert de messages
- **PCI** : Peripheral Component Interconnect (PCI) est un standard de bus local (interne) permettant de connecter des cartes d'extension sur la carte mère d'un ordinateur.
- **PCI/DSS :** Payment Card Industry Data Security Standard
- **Plug-and-Play** : une procédure permettant aux périphériques récents d'être reconnus rapidement et automatiquement par le système d'exploitation dès le redémarrage après l'installation matérielle.
- **Ponemon Institute :** un cabinet spécialisé dans la gestion et la confidentialité des informations.
- **RAM** : Random Access Memory la mémoire informatique dans laquelle un ordinateur place les données lors de leur traitement.
- **SMTP** : Simple Mail Transfer Protocol
- **SQL** : Structured Query Language est un langage informatique normalisé qui sert à demander des opérations sur des bases de données.
- **Telnet :** un protocole permettant d'émuler un terminal à distance
- **USB :** Universal Serial Bus
- **WCF** : un sous-système de communication(Indigo). Les applications WCF peuvent être développées en utilisant les différents langages de Microsoft .NET

Introduction Générale

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique.
La sécurité recouvre ainsi plusieurs aspects :

- intégrité des informations (pas de modification ni destruction)
- confidentialité (pas de divulgation à des tiers non autorisés)
- authentification des interlocuteurs (signature)
- respect de la vie privée (informatique et liberté).

Des données financières, fiches clients, éléments de propriété intellectuelle, voire les dossiers de salariés échappent au contrôle des entreprises. Bien souvent, les coupables ne sont même pas des pirates informatiques, mais des membres de personnel. Qu'elles soient le fait d'erreurs humaines ou de vols qualifiés, les fuites d'informations surviennent la plupart du temps via des canaux de diffusion courants (messagerie électronique, publication web, enregistrement sur clés USB, impression) et peuvent se solder par des pertes financières chiffrées en millions.

Le logiciel McAfee Host DLP protège les entreprises contre les risques associés aux transferts non autorisés de données, à l'intérieur ou à l'extérieur de l'entreprise. L'expression « fuite de données » implique la diffusion au-delà des frontières de l'entreprise d'informations de nature confidentielle ou privée, à la suite d'une communication non autorisée via divers canaux de transfert.
C'est dans ce cadre que s'inscrit mon Projet de Fin d'Etudes effectué au sein de la société CBI. Ce projet consiste en la réalisation d'une maquette de test de la solution McAfee Host data loss prevention. Il m'a été indispensable de maîtriser cette technologie, tant au niveau théorique qu'au niveau pratique.

Dans ce rapport, je commencerai tout d'abord par une présentation de l'organisme d'accueil, CBI, le premier chapitre qui présente une vue générale sur le domaine de prevention contre les fuites de données. Le second chapitre sera axé principalement sur les différentes solutions présentes dans le marché. Le troisième chapitre consacrera pour une étude comparative entre les différentes technologies. Le quatrième chapitre est focalisé sur la présentation de la solution McAfee Host DLP, Le dernier chapitre va décrire les différentes étapes de conception, d'installation et de configuration que j'ai suivie pour la mise en œuvre de la maquette.

Chapitre I : Organisme d'accueil et Principe de DLP

1. Organisme d'accueil

CBI (Compagnie Bureautique Informatique) est une entreprise privée à capital marocain. Elle a été fondée en 1970. Le siège principal à Casablanca. Elle compte plusieurs agences à Rabat, à Tanger, à Agadir, à Marrakech, à Fès et au Sénégal.

C'est une entreprise à activités variées dans le domaine des nouvelles technologies. Celle des solutions, qui couvrent des produits et des marchés complémentaires (bureautique, informatique, systèmes d'information, télécommunications, Internet/Intranet) et toujours, présente des nouvelles technologies et des outils de productivité. Les principales activités de la société CBI sont :

- Audit,
- Conseil informatique,
- Conception d'architectures réseaux,
  - LAN / WAN,
  - Data, téléphonie IP et vidéoconférence,
  - Transmissions Radio et Laser,
  - Gestion de réseaux / Supervision de réseaux,
  - Sécurité.
- Implémentation,
- Formation professionnelle,
- Maintenance / Support technique.

Avec un capital de 15.000.000 DH et des collaborateurs actifs (450 de personnels), la CBI a su s'imposer dans le marché des réseaux informatique et susciter la confiance des grandes entreprises telles que, BMCE, BMCI et CISCO.

La société CBI contient plusieurs départements (Image multimédia, Formation, DataCom, et autres). Le présent stage a été effectué au sein du département « Télécommunication » au service support technique.

Rapport-Gratuit.com

A l'ère de l'information, «prévenir les pertes» n'est plus limité à la réduction des malversations dans la chaîne d'approvisionnement, le commerce ou l'administration. Désormais, le savoir-faire d'une entreprise se trouve surtout dans des bases de données, emails ou fichiers et non dans des caisses en cartons, entrepôts ou classeurs. Depuis les listes clients, les factures, les déclarations financières jusqu'aux produits et projets d'ingénierie, les organes vitaux d'une entreprise résident autant dans les données électroniques, les réseaux informatiques et les ordinateurs portables dans les bureaux, magasins, usines, sa valeur ajoutée repose sur sa facilité d'utilisation à travers toute l'entreprise.

Tant que beaucoup d'attention a été accordée à la protection des actifs des entreprises contre les menaces extérieures provenant des systèmes de prévention d'intrusion de pare-feu , les organisations de gestion des vulnérabilités doivent maintenant porter leur attention sur une situation aussi dangereuse a savoir le problème de perte de données de l'intérieur.

Pour relever ces challenges, une nouvelle technologie est apparue : la Prévention contre la fuite de Données .Elle offre une nouvelle analyse de l'utilisation de l'information et applique des contrôles de protection pour prévenir les incidents indésirables.

Compte tenu aujourd'hui de la prévention de réglementation et de l'environnement ultra-concurrentiel, la perte de données est l'un des enjeux les plus importants. Pour ceux qui créent et mettre en œuvre une stratégie de DLP, la tâche peut sembler difficile.

2. Constats, Risques & Enjeux

La création et le partage de l'information numérique au sein des entreprises continues à accéléré. Cependant, les technologies mêmes (e-mail, Web, messagerie instantanée, etc) qui permettent ce niveau avancé de la connectivité et la collaboration entre employés, clients, partenaires génère également un énorme risque de sécurité pour les entreprises qui les utilisent. Une seule "initiés" violation de données sensibles, que ce soit par des effets intentionnels ou carrément malveillants, peut exposer l'entreprise à grande portée financière, les relations publiques, services juridiques, et la réputation.

Une enquête révèle que 93 % des professionnels de la sécurité estiment que les sociétés subissent une pression accrue quant à la protection contre les pertes de données. La menace interne a été mise en évidence comme facteur clé, avec 73 % des sondés attribuant la perte de données à des collaborateurs quittant l'entreprise avec les données en question. La technologie de prévention contre la fuite de données peut servir à garantir que les collaborateurs se conforment aux mesures de sécurité des politiques concernant les données, assurant la protection des données les plus confidentielles des entreprises

Les études de Gartner, Forrester, FBI, Ponemon Institute montrent que :

- 1 message sur 400 contient des données confidentielles
- 1 fichier sur 50 est partagé à tort
- 1 ordinateur portable sur 10 est volé
- 1 clé USB sur 2 contient de l'information confidentielle

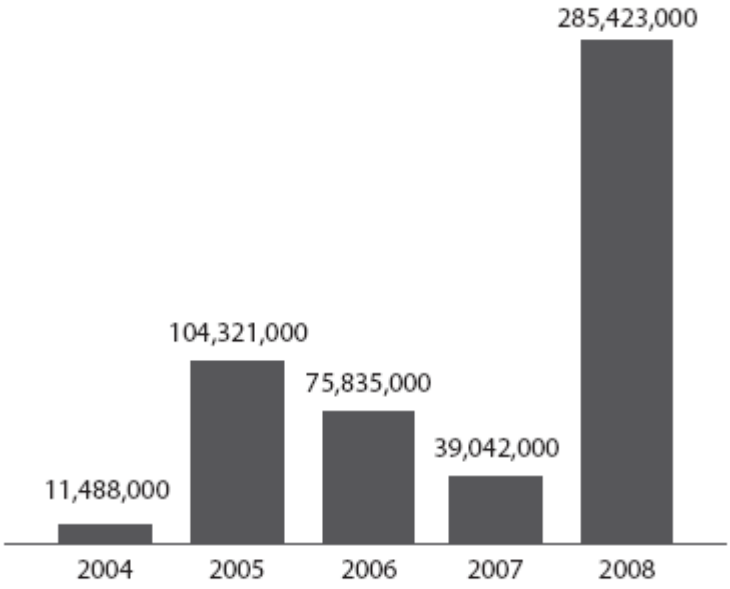


Figure : 1 Nombres de violations par an : Source Verizon 2009 Data Breach Investigations Report

Selon l'étude Ponemon Institute réalisée au Royaume-Uni en février 2008, le coût d'une fuite pourrait aller de 100.000 à 5 millions d'euro. 36% des coûts seraient dus à des pertes commerciales, suites à des départs de clients particulièrement. 36% des pertes seraient liées à des vols de portables aux autres appareils mobiles. Dans tous les cas, ces pertes d'informations causent aussi des préjudices en termes d'images aux entreprises qui en sont victimes.

Donc l'information est l'un des atouts les plus importants d'une entreprise. Les entreprises veulent être en mesure d'accéder aux informations de n'importe où, sur n'importe quel appareil, et de collaborer avec presque tout le monde. Le désir d'information à être "libre" de sécurité présente de nombreux défis et de gestion des risques. Les organisations ont déménagées de la sécurisation de l'infrastructure IT d'obtenir des renseignements.

3. Qu'est-ce que le DLP ?

DLP signifie « Data Loss Prevention » Prévention contre la fuite de données. La DLP permet aux entreprises de concevoir, exécuter et distribuer une politique de sécurité efficace des flux d'informations afin de garder un contrôle sur les données critiques (propriété intellectuelle, données personnelles, données financières, code source, …). Il permet également à l'entreprise de se conformer aux politiques de sécurité internes ou réglementaires et de faciliter le partage d'informations en toute sécurité pour ses utilisateurs nomades munis de PCs portables ou autres périphériques mobiles. La DLP se focalise sur la sécurisation de la donnée tout au long de son cycle de vie et s'applique donc aux données en transit (données quittant le réseau via email ou trafic web), aux données en cours d'utilisation (données en cours d'impression, copie sur clés USB ou autres médias transportables…) et aux données au repos (données stockées ou archivées).

Rapport gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

On peut dire que DLP c'est une solution basée sur des règles centralisées qui identifie, surveille et protège les données qu'elles soient stockées, en cours d'utilisation ou en mouvement quel qu'en soit le support.
Donc cette définition résume les principaux modules d'une solution DLP : gestion centralisée, identification et définition de l'information, contrôle de son utilisation et protection contre les infractions.

4. Sources des violations de données

À un niveau élevé, les incidents de sécurité proviennent d'une seule ou une combinaison des sources suivantes:

- Externe :

Les menaces extérieures proviennent de sources situées en dehors des organisations. Les exemples incluent les pirates, les groupes du crime organisé, ainsi que les événements environnementaux comme la météo et les tremblements de terre. En règle générale, pas de confiance ou de privilège est implicite pour les entités externes.

- Interne

Les sources menace sont ceux qui proviennent de l'intérieur des organisations. Cela englobe les cadres de l'entreprise, les employés et les stagiaires. La plupart des initiés ont la confiance dans une certaine mesure et certains, les administrateurs informatiques en particulier, ont des niveaux élevés d'accès et de privilège.

- Partenaires

Les partenaires comprennent un tiers partageant une relation d'affaires avec les organisations. Cette chaîne de valeur des partenaires, les fournisseurs, les entrepreneurs et les clients est connue sous le nom de l'entreprise étendue. L'échange d'informations est l'élément vital de l'entreprise étendue, et pour cette raison, un certain niveau de confiance et de privilège est habituellement implicite entre partenaires d'affaires

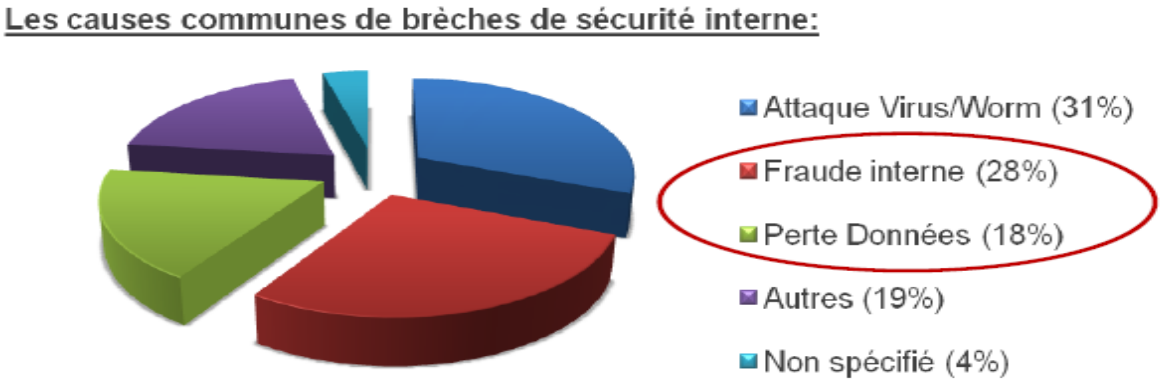


Figure 2 : Les causes communes de brèches de sécurité interne D'après "Deloitte'sGlobal Security Survey"

5. Fonctionnement de DLP

Plutôt que d'aborder la technologie d'un composant spécifique, classons les différentes architectures de la DLP en fonction du type de protection qu'elles proposent : l'information en mouvement pour les emails et les autres communications réseaux, l'information stockée pour les données «statiques» et l'information traitée pour les données transmises d'un ordinateur vers une clé USB par exemple. Derrière tout cela se trouve le serveur de gestion centralisée, où les politiques sont définies et les incidents gérés.

5.1 Les données en mouvement

Quand on discute de DLP, on utilise l'information en mouvement pour décrire la circulation du contenu dans les différents réseaux (email, activité sur le web, messagerie instantanée…). Trois modules entrent alors en fonction pour contrôler et protéger cette information :

- Contrôleur Réseau : une Appliance ou un serveur chargé de scanner le réseau afin de localiser et de contrôler l'information. En général, il s'agit d'un scan passif (simple surveillance des données) mais certains outils prennent action et bloque les infractions à la politique de l'entreprise. La plupart des solutions DLP peuvent aussi collaborer avec les passerelles web existantes afin de stopper toute activité indésirable (dont certaines cryptées).

- Email : l'email est un peu différent des autres circulations d'information. En termes de besoin de protection, c'est le plus important. Et la façon dont l'email fonctionne offre de nombreuses options : redirection automatique d'emails sensibles vers un responsable par exemple, afin d'en autoriser l'envoi.

- Agent logiciel pour poste de travail : dans chaque organisation, il y a des employés qui se connectent à l'Internet depuis l'extérieur, en dehors du réseau de l'entreprise (à la maison ou dans des cybercafés). Un agent logiciel sur leurs ordinateurs portables peut contrôler leur activité réseau.

En pratique, le contrôleur réseau et l'agent logiciel sont souvent associés sur le serveur de gestion centralisée mais peuvent aussi être indépendants pour les entreprises plus importantes ou décentralisées. Les agents logiciels placés sur les ordinateurs portables protègent les informations stockées et traitées.

5.2 Les donnes stockées

Une des caractéristiques les plus notables d'une solution DLP est sa capacité à analyser minutieusement l'information stockée afin de détecter les données sensibles.

Localiser dans l'instant tous les emplacements de stockage des données clients, ordinateurs portables et serveurs non autorisés inclus, est une valeur ajoutée à considérer.

Trois modules existent pour gérer l'information stockée :

• balayage à Distance : La solution DLP se connecte au répertoire de stockage, de la même façon qu'un utilisateur le ferait à la recherche d'un ficher. Ensuite la solution scanne tous les fichiers et analyse les données sensibles.

•Agent logiciel local : Le balayage à distance utilise la bande passante du réseau et bien qu'il puisse atteindre les utilisateurs n'importe où, ce n'est pas la meilleure méthode. Pour des répertoires de stockage important, on peut installer un agent logiciel plus efficace capable de scanner l'information localement pour ensuite communiquer les résultats de l'analyse au serveur central. Les agents logiciels sont aussi préférables pour contrôler et protéger les fichiers des ordinateurs des employés.

•Intégration d'application : Certaines entreprises utilisent des solutions de gestion de contenu telles que Microsoft SharePoint et EMC Document. L'intégration parfaite des solutions DLP avec ces outils permet de tirer parti de leurs fonctionnalités.

5.3 L'information traitée

Les agents logiciels servent à identifier, contrôler et protéger l'information en mouvement et stockée sur les ordinateurs des employés. Ces agents peuvent aussi protéger l'information traitée. Par exemple : des utilisateurs cherchant à déplacer des données ou fichiers sensibles vers un emplacement de stockage portable, en utilisant des applications non autorisées.

5.4 Gestion centralisée

La solution DLP se concentre sur les problèmes métier (protéger l'information sensible) et non sur les problèmes techniques, il est donc important pour les produits DLP d'être accessibles à ces deux communautés d'utilisateurs. La création de politiques ne doit pas exiger de connaissances informatiques trop poussées et la gestion d'un incident doit être à portée de main d'une ressource « Conformité », « Risque » ou « Ressources Humaines ».

5.5 L'analyse de contenu

Une analyse approfondie du contenu est la caractéristique principale d'une solution de Prévention contre la fuite de Données. C'est de cette façon qu'une solution DLP identifie l'information sensible, qui est ensuite comparée avec la politique interne de l'entreprise pour assurer son application.

Il y a deux étapes dans l'analyse de contenu : la division des fichiers pour atteindre l'information et l'analyse. Cinq techniques principales d'analyse de contenu sont proposées mais leur disponibilité et leur efficacité se diffèrent de produit à un autre.

• Politiques : la solution DLP recherche l'information qui correspond au modèle prédéfini, tel que la structure d'une carte de crédit ou le numéro de Sécurité Sociale.

• Concordance de base de données : la solution DLP se connecte à une base de données et détecte ensuite le contenu issu de cette base uniquement ; des coordonnées de clients par exemple.

• Statistiques : La solution DLP utilise des analyses de statistiques pour identifier le nouveau contenu similaire aux sources déjà connues.

• Conceptuel : le système consulte les politiques et les dictionnaires prédéfinis pour localiser le contenu ayant un thème spécifique.

• Catégories : Des catégories sont créées pour les types de données sensibles les plus courants, rapports financiers par exemple.

La majorité des solutions DLP autorisent la combinaison de différentes techniques d'analyses en une politique unique.

La Prévention contre la Perte de Données est un outil puissant capable de protéger le patrimoine numérique. La DLP n'est pas parfaite et ne peut contrer toutes les erreurs ou agressions mais c'est un outil efficace apte à réduire les coûts liés à la conformité, les risques de perte de données et les infractions.

6. Les avantages principaux du DLP ?

En utilisant la DLP, les organisations peuvent contrôler de manière centralisée les flux de données et empêcher toute fuite d'information, accidentelle ou intentionnelle. La DLP permet de renforcer les processus de sécurité grâce à ses caractéristiques suivantes :

- Centralisation de la politique de sécurité

La sécurité et la conformité des flux d'informations ne dépendent plus des utilisateurs finaux. La solution DLP découvre, classifie, applique les règles et signale de manière centralisée, sans intervention de l'utilisateur. Dans de nombreux cas, la DLP distribue la responsabilité en matière de protection des données à plusieurs niveaux de l'organisation.

- Gestion des menaces internes

L'extension et la pénétration des outils NTIC les positionnent au rang des premiers outils de vengeance. Détruire un PC, détruire un serveur, partir avec des informations confidentielles (base de données clients…) sont malheureusement des fraudes courantes. Par leur capacité de détection, classification, contrôle et signalement des données sensibles, les solutions DLP peuvent limiter de nombreuses incivilités informatiques aux conséquences souvent fâcheuses.

- Mobilité améliorée et sécurisée

Un accès distant sécurisé et disponible en permanence représente un défi majeur et un avantage concurrentiel considérable pour toute entreprise. Disposer d'utilisateurs productifs et capables de réagir avec souplesse et rapidité aux exigences du marché représente un véritable avantage. La DLP, en sécurisant l'accès aux données et en contrôlant leur

circulation améliore la sécurité globale de l'entreprise étendue, quels que soient les scénarios d'usage et de connexion des utilisateurs aux données critiques.

7. Conclusion

La prévention des pertes de données est un problème grave pour les entreprises, comme le nombre d'incidents (et le coût pour ceux qui connaissent eux) continue d'augmenter. Qu'il s'agisse d'une tentative malveillante, ou une erreur involontaire, la perte de données peut réduire la marque d'une entreprise, de réduire la valeur actionnariale, et des dommages de bonne volonté de l'entreprise et sa réputation.

Donc les entreprises peuvent rechercher une solution de prévention des pertes de données qui s'adapte le mieux à leurs besoins particuliers. Pour la conformité aux règlements tels que HIPAA (Health Insurance Portability and Accountability Act) et PCI, la protection de la propriété intellectuelle, et l'exécution des politiques d'utilisation appropriée.

La protection contre les fuites de données est aujourd'hui un impératif stratégique en raison des risques potentiels de pertes financières, de dégradation de la confiance de la clientèle et de dommages à l'image de marque qui sont tout simplement trop importants pour pouvoir être négligés. Il n'en reste pas moins que la définition d'une stratégie de sécurité et son implémentation ne sont jamais des tâches triviales.

Chapitre II: Etude et présentation des différents acteurs du marché

De nombreux fournisseurs assurent d'être présents sur le marché du DLP (Data Loss Prevention), qui lutte contre la fuite d'informations. Mais les solutions qui traitent ce genre de problèmes sont rares. La technologie semblerait mature si l'on se réfère à l'âge des principaux outils, nés il y a pas longtemps. Mais ces produits émanaient de petits éditeurs récemment rachetés par les leaders, qui ne les ont pas encore tous intégrés dans leurs gammes.
RSA (division d'EMC), Symantec, McAfee et Websense ont ainsi respectivement absorbé Tablus, Vontu, Reconnex et Port Authority. Cisco ajoute pour sa part des fonctions de DLP dans ses produits et Microsoft vient de s'associer à RSA. Enfin, Code Green Networks est l'un des rares spécialistes encore indépendants.

Bien que cela varie d'un fournisseur à un autre, il y a généralement trois niveaux différents d'une solution DLP dépend de type de donnes soit des données au repos (poste de travail), les données en mouvement (réseaux) et les données stockage (serveurs).par la suite je vais vous présenté les différents fournisseurs qui opèrent dans le domaine de DLP.

Un grand investisseur a un jour déclaré qu'il fallait vingt ans pour se forger une réputation, mais que cinq minutes suffisaient à la détruire. Lorsque des services informatiques protègent les données sensibles d'une entreprise contre la perte ou un usage abusif, ils contribuent par la même occasion à préserver son image et sa réputation. Chaque société dispose de données sensibles qui sont indispensables à son fonctionnement. Il s'agit, par exemple, de données financières, d'informations relatives aux clients, de brevets et de formules de produit. L'utilisation appropriée de ces informations étant essentielle pour le fonctionnement de la société, il convient de les protéger contre diverses formes de perte et d'usage abusif.

1. CA DLP (Orchestria)

CA DLP c'est un Système efficace de protection des données, qui permet aux organisations de mieux protéger et contrôler ces données critiques là où elles sont utilisées et stockées, réduisant ainsi les risques associés à des informations non contrôlées et les aidant à se conformer aux directives réglementaires et à leurs politiques de confidentialité tout cela par utilisation des identités pour analyser l'activité des utilisateurs finaux en temps réel et interpréter les données avec un haut niveau de précision.

Elle est conçue pour offrir un vaste éventail de fonctionnalités qui aident les organisations à atteindre leurs objectifs de prévention de la fuite de données et de protection des informations. Parmi les fonctionnalités on site :

- **Couverture de protection complète** : compte tenu de la divergence des besoins et priorités, CA DLP est conçu pour protéger les données là où c'est nécessaire, à savoir point à sécuriser, serveur de messagerie, réseau et système de stockage.

- **Identification des divers types de données** : les données nécessitant une protection peuvent être de plusieurs types. CA DLP prendre toutes en charge.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

- **Règles prédéfinies flexibles** : les règles prédéfinies configurables de CA DLP s'appuient sur les meilleures pratiques du secteur pour identifier précisément et protéger les données sensibles.

- **Evolutivité et résilience de l'entreprise** : CA DLP peut être déployé sur des milliers de PC et permet d'analyser des téraoctets de données.

- **Actions de contrôle appropriées** : Les actions disponibles incluent le blocage, l'avertissement, la mise en quarantaine, la redirection, le déplacement, la suppression, le remplacement, la capture et l'alerte.

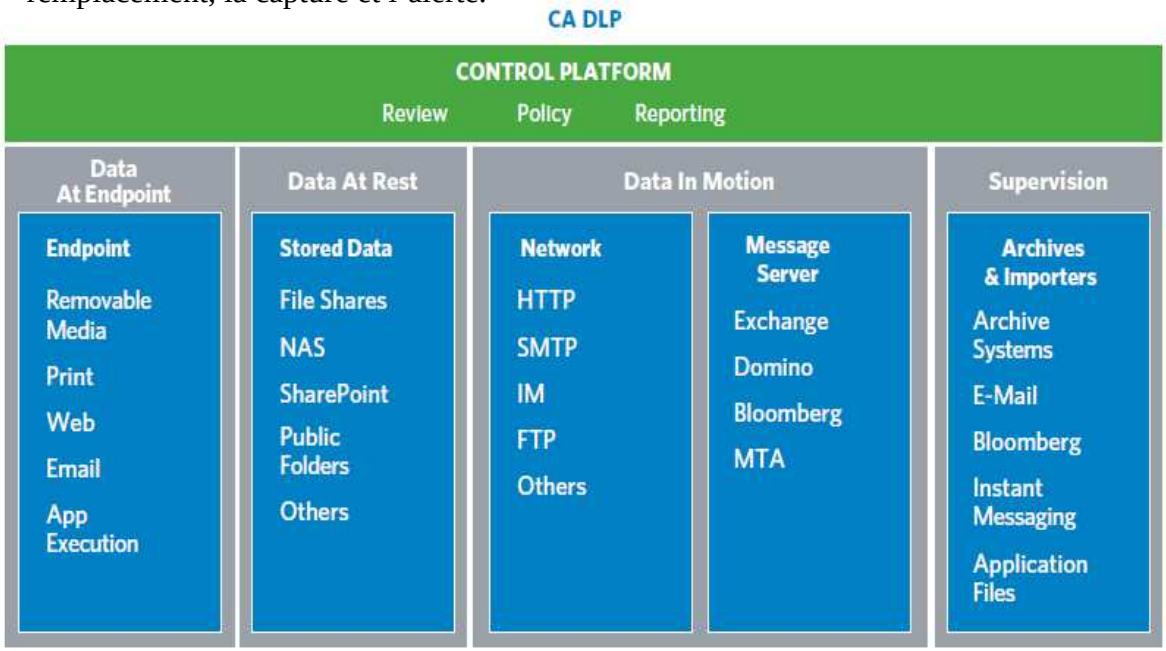


Figure : 3 Plateforme CA DLP

CA DLP est une des solutions de sécurité éprouvées de CA qui aide à protéger les ressources informatiques sur de nombreux environnements et plates-formes. Ce composant contribue ainsi à l'optimisation des performances, de la fiabilité et de l'efficacité de l'environnement informatique global.

2. EMC/RSA

La suite de prévention des fuites de données RSA DLP (Data Loss Prévention) permet de réduire l'ensemble des risques auxquels les données sensibles sont confrontées : qu'elles soient statiques dans un « Data Center », en mouvement dans le trafic réseau ou extraites par un utilisateur final à l'un de ses points de terminaison.

Les trois produits de la suite RSA DLP (RSA DLP Datacenter, RSA DLP Network et RSA DLP End point) capitalisent sur un système unifié de gestion des politiques pour simplifier leur

déploiement dans un environnement homogène et cohérent de gestion de l'intégralité des données sensibles d'entreprise.

- **Les produits RSA DLP**

La Suite RSA DLP est constituée de trois produits intégrés offrant une approche proactive de la gestion des risques métier liés aux fuites de données : RSA DLP Datacenter, RSA DLP Network et RSA DLP End point (commercialisés séparément ou sous forme de package complet en fonction des objectifs spécifiques de client).

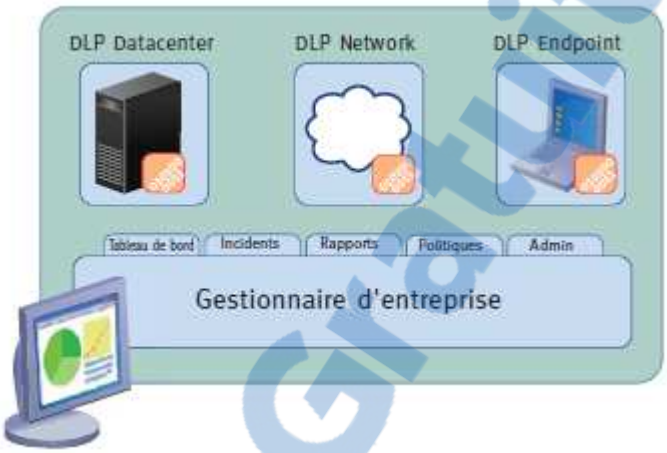


Figure : 4 Plateforme RSA® DLP

- **RSA® DLP Datacenter**

Data Center a pour vocation d'exécuter et supporter les applications des différentes unités métier de l'entreprise. Ils manipulent donc généralement de grandes quantités de données, dont une partie est naturellement sensible et répartie entre différents systèmes de fichiers, bases de données, systèmes d'e-mail et de gestion de contenus ou environnements de stockage étendus (SAN/NAS). RSA DLP Datacenter découvre les données sensibles à travers une analyse détaillée et offre une vision synthétique des risques encourus.

- **RSA® DLP Network**

La collaboration aussi bien interne qu'externe est critique pour le succès des entreprises et dans l'économie actuelle elle passe par des échanges par email, messagerie instantanée et autres formes d'échanges réseau. Intentionnellement ou non, un fichier sensible peut en effet quitter l'entreprise attaché à un e-mail ou un secret commercial être dévoilé par messagerie instantanée.

La vocation RSA DLP Network est de réduire ces risques grâce à sa capacité à détecter et analyser rapidement et avec précision les données quittant le réseau et à appliquer des politiques de sécurisation des données basées sur le type d'activité et les politiques de sécurité.

Rapport-Gratuit.com

Donc RSA DLP Network a pour rôles principales de :

- Contrôle passif des données sensibles circulant sur le réseau.
- Blocage actif et correction des données en mouvement en fonction de politiques.
- Émission d'alertes de notification.

- **RSA DLP End point**

Les points de terminaison réseau (stations de travail, ordinateurs portables, etc.) ont révolutionné la conduite des affaires au quotidien et jouent un rôle critique pour maximiser la réussite, la productivité et la mobilité des collaborateurs. Ces derniers passant la plupart de leur temps de travail sur ces « points de terminaison », rien d'étonnant à ce que leurs PC recèlent tôt ou tard de grandes quantités d'informations sensibles. Les statistiques sont d'ailleurs édifiantes que plus de 50 % des données perdues dans les environnements informatiques modernes proviennent de ces points de terminaison via des transmissions hors ligne vers des périphériques mobiles.

RSA DLP End point découvre et analyse les données sensibles hébergées par les portables et postes de travail. Puis, il en renforce la sécurité en bloquant la transmission des données sensibles hors ligne vers des supports mobiles tels que clé USB, CD, DVD, et en appliquant des contrôles supplémentaire sur l'impression.

3. Symantec DL

Symantec Data Loss Prevention une solution unifiée pour la recherche, la surveillance et la protection des informations confidentielles, quel que soit l'endroit où elles sont stockées ou utilisées. Symantec assure une protection complète des données confidentielles sur les terminaux, les réseaux et les systèmes de stockage. En réduisant les risques de manière quantifiable, il propose de nouveaux moyens pour prouver la conformité de l'entreprise tout en protégeant les clients, la marque et la propriété intellectuelle.

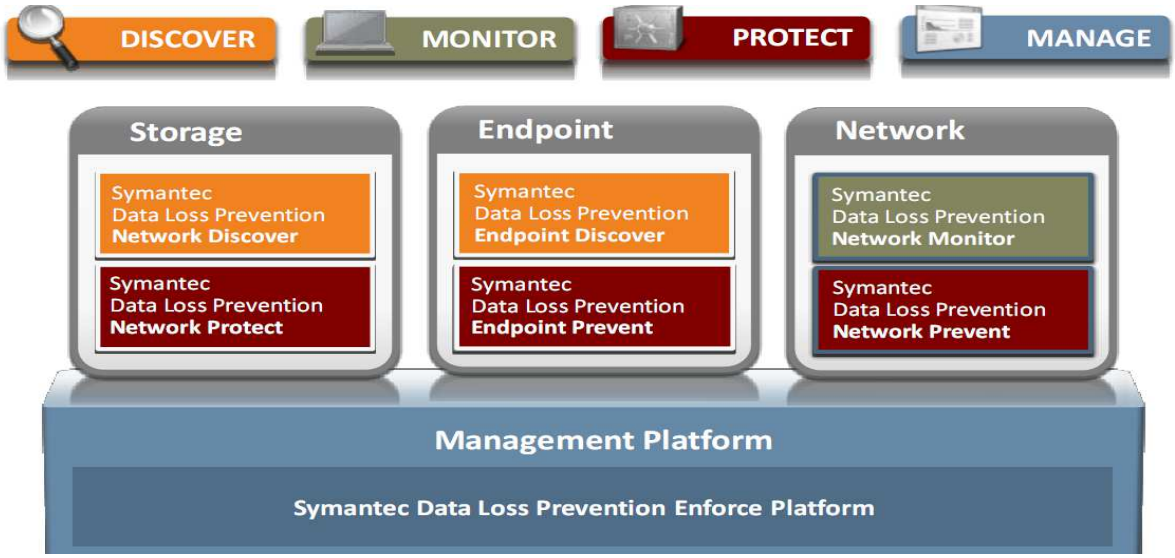


Figure 5 : Plateforme Symantec DLP

- **Avantages clés**

- Réduction de la dispersion des données confidentielles dans les data center, les systèmes clients, les bureaux distants et les ordinateurs des utilisateurs.
- Identification des processus défaillants qui permettent la transmission de données confidentielles.
- Surveillance et protection des communications de contenus sensibles vers les sites Web publics.
- Définition et déploiement de politiques homogènes dans l'entreprise.

Les services de prévention des fuites de données de Symantec permettent aux clients de tirer pleinement profit de leur solution DLP et d'acquérir les connaissances et l'expérience requises pour son optimisation permanente au fil du temps. En combinant des services de conseil et des technologies leaders de prévention des fuites de données, elle fournit un rapport détaillé sur l'exposition aux risques de vol de données internes et externes, ainsi qu'une évaluation quantitative des fuites de données effectives au niveau des réseaux, du stockage des applications Web et des points d'accès.

4. Vericept

Vericept fournit aux entreprises une solution complète de prévention des fuites de données qui découvre, classifie et protège les informations sensibles en mouvement, au repos et encours utilisation. Vericept découvrir automatiquement des informations sensibles en temps réel. Après la découverte, Vericept classifie et protège les informations critiques contre la diffusion non autorisée, même lorsqu'ils sont modifiés. Donc la solution Vericept permet aux entreprises d'atténuer les violations de la conformité réglementaire, perte de propriété intellectuelle.

- **Composants de la prévention de perte de données**

Offrir une visibilité complète de l'entreprise, la Solution Vericept Data Loss Prevention est une plate-forme intégrée composée de quatre éléments principaux pour une protection maximale des données précieux.

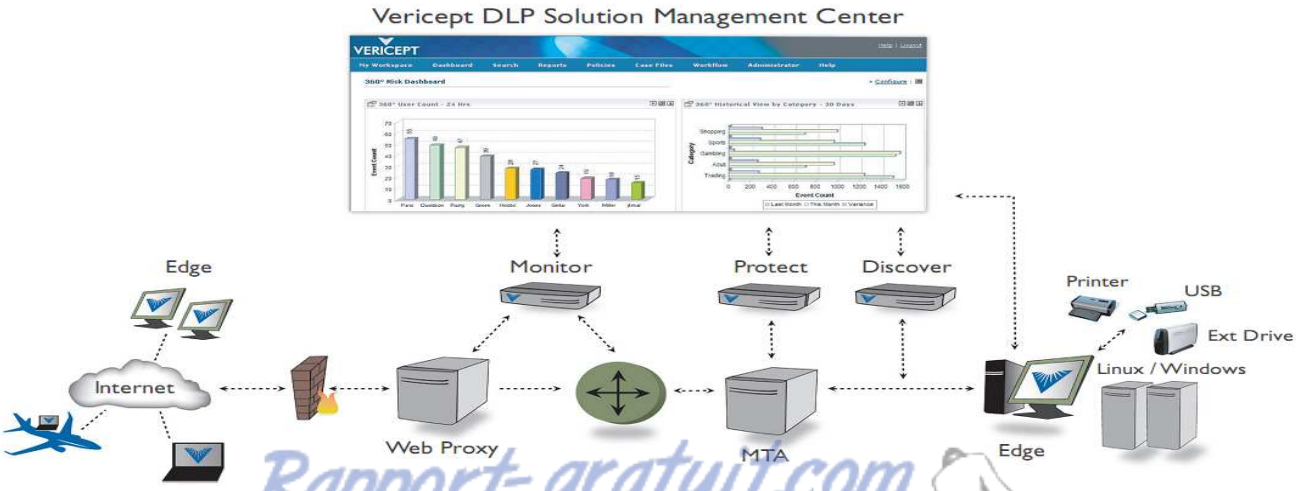


Figure 6 : Architecture de Vericept DLP

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

- **Vericept monitor**

Basé sur une suite de classement des brevets en instance, la solution du moniteur de Vericept analyse tous les communications et attachements basés sur Internet comprenant l'email, IM, messagerie instantanée, les blogs, le ftp et le Telnet contre les violations du données de l'entreprises.

- **Vericept Protect**

Vericept Protect permet de contrôler email pour se défendre contre une fuite non autorisée de données. Les communications par courriel et les pièces jointes sont analysés et peuvent être automatiquement chiffrés, bloqué, mis en quarantaine.

- **Vericept discover**

Vericept discover analyse des données au repos pour trouver des violations résidé dans les données stockées sur des bureaux, des ordinateurs portables et des serveurs. Basé sur la suite de classification de Vericept, il analyse des données au repos utilisant les catégories de risque de Vericept pour identifier et capturer des violations de la politique de corporation et de conformité, et pour fournir l'éléments de preuve. Lorsqu'une infraction est signalée, Vericept peut crypter automatiquement les informations pour se protéger contre une utilisation non autorisée.

- **Vericept Edge**

Vericept Edge contrôle des fuites d'informations sur les ordinateurs de bureau et aux extrémités. Edge permet aux organisations de découvrir des données confidentielles sur les portables, ordinateurs de bureau et serveurs afin de déterminer tous les risques d'initiés et les infractions associées à la fuite de données et les violations confidentiels conformité. Prévenir la fuite d'informations confidentielles aux points finaux peuvent être appliquées en limitant la possibilité d'imprimer, enregistrer, copier, d'accès, de circulation et de télécharger des données sensibles sur des supports amovibles ou autres lecteurs qu'il soit connecté ou déconnecté du réseau.

Vericept fournit une interface utilisateurs qui facilite la gestion de politique et le workflow. Les écrans d'événement sont personnalisables, permettant à des utilisateurs de définir facilement la manière que l'information d'événement est montrée. Une interface graphique de tableau de bord permet la mise en place politique simple fondée sur l'inclusion / exclusion, la surveillance basée sur le temps et d'administration en un seul clic.

5. Websense

Les technologies de prévention de fuites de données (DLP) de Websense® font partie de la solution de Websense TRITON™, cette technologie conçues pour fixer les informations sensibles et la propriété intellectuelle, ainsi que gérer et faire respecter les exigences réglementaires

La solution Websense Data Loss Prevention est une plate-forme intégrée composée de quatre éléments principaux pour assuré une protection maximale des données :

- Moniteur informatique de Websense

Websense Data Monitor ® est une solution réseau DLP pour surveiller les données. Elle fournit la possibilité d'identifier automatiquement quelles sont les données client à risque; qui utilise les données en temps réel, et où ces données se passe sur le Web.

- Websense protect

Websense ® Data Protect met l'accent sur la protection des données confidentielles sur le réseau, puisque le principal risque de fuites de données est l'utilisation abusive ou la divulgation non autorisée de données confidentielles.

- Data Discover

Websense ® Data Discover une solution logicielle qui scanne à distance de partages de fichiers réseau, bases de données, serveurs de messagerie, les référentiels de données et ordinateurs de bureau à découvrir et à classer les données confidentielles sur ces systèmes. Il appliquer automatiquement les politiques de protection des données sur ces systèmes par l'application des mesures y compris le cryptage, la notification, la vérification et l'enregistrement des violations.

- Data End point

Websense ® Data End point reprend là où la prévention des fuites de données réseau (DLP), en fournissant la sécurité des terminaux et de contrôle sur les données confidentielles et doivent être conservés, comment il est utilisé, où il est transféré (stockage USB, imprimante), et l'action en temps réel afin de prévenir la fuite de données.

La suite de protection des données de Websense inclut les quatre modules intégrés, contrôlés sous un cadre de politique simple. Elle offre la visibilité et le contrôle de la fuite de données de réseau et de point final ainsi que la découverte de données globale sur les systèmes de stockage des organisations.

6. McAfee Data Loss Prevention

Le comportement de certains utilisateurs peut mettre en péril les données confidentielles des entreprises ce qui provoqué des conséquences désastreuses. Les solutions McAfee Data Loss Prevention surveille et prévient les comportements à risque, susceptibles d'entraîner des divulgations de données sensibles. Cette protection s'étend aux applications, aux périphériques de stockage amovibles et aux réseaux. Que l'employé en possession des données soit au bureau, chez lui ou en déplacement.

- **Composants de McAfee Data Loss Prevention**

- McAfee Host Data Loss Prevention

McAfee Host DLP logiciel permet de surveiller et de prévenir immédiatement la perte de données confidentielles au travail et en dehors de l'entreprise. McAfee Host DLP protège les

entreprises contre les risques de perte , les dommages de la marque, perte de clients.il permet la surveillance des événements en temps réel, l'application des politiques de sécurité à gestion centralisée pour contrôler la façon dont les employés utilisent et le transfert de données sensibles , et de générer des rapports détaillés avec un impact minimal sur les activités quotidiennes. Il empêche également la perte de données et les fuites lorsque les données sont modifiées, copiées, collées, imprimés, ou transmis, tout en permettant une utilisation flexible.

- McAfee Network DLP Discover

McAfee Network Data Loss Prevention Discover permet la vérification le cas ou les données sensibles sont menacées et de savoir où elles ont été distribuées. Il peut même identifier des données sensibles complexes, telles que les informations relatives à la propriété intellectuelle, qui sont plus difficiles à définir que les données fixes, telles que les numéros de carte de crédit ou de sécurité sociale.

- McAfee Network DLP Prevent

McAfee Network DLP Prevent prévient les fuites de données intentionnelles ou non, en permettant aux entreprises d'empêcher de façon proactive leurs informations confidentielles de quitter le réseau et de mettre en œuvre les processus appropriés. Les stratégies concernant les mouvements d'informations sont mises en œuvre quel que soit le moyen de transfert (e-mail, messagerie web, messagerie instantanée, wikis, blogs, portails, HTTP/HTTPS et FTP), en s'intégrant à des passerelles de type agent de transfert de messages (MTA) à l'aide du protocole SMTP (Simple Mail Transfer Protocol) ou de proxy web ICAP (Internet Content Adaptation Protocol). Si une infraction à la stratégie est détectée, elle permet de prendre diverses mesures, telles que le chiffrement, le blocage, la mise en quarantaine et la redirection, entre autres. Les violations de la sécurité sont réduites et la conformité aux règlements de confidentialité est assurée.

- McAfee Network DLP Monitor

McAfee Network DLP Monitor permet de rassembler et suivre les données en mouvement dans l'ensemble de réseau en temps réel, et générer des rapports sur ces données. Egalement il permet de savoir quelles informations circulent entre les utilisateurs et les autres entreprises, et de quelle manière. Appliance unique et spécialisée de haute performance, qui détecte plus de 300 types de contenu traversant tout port ou protocole, McAfee Network DLP Monitor peut aider à découvrir les menaces qui pèsent sur les informations et à prendre des mesures pour protéger les entreprises des fuites de données.

- McAfee Network DLP Manager

Avec McAfee Network DLP Manager, présente une vue unique sur toutes les Appliance McAfee Network DLP et les agents hôtes distribués sur tout le réseau. Les applications d'apprentissage McAfee DLP Network permettent ainsi de minimiser le temps et les coûts associés à la compréhension et à la protection de données confidentielles

.

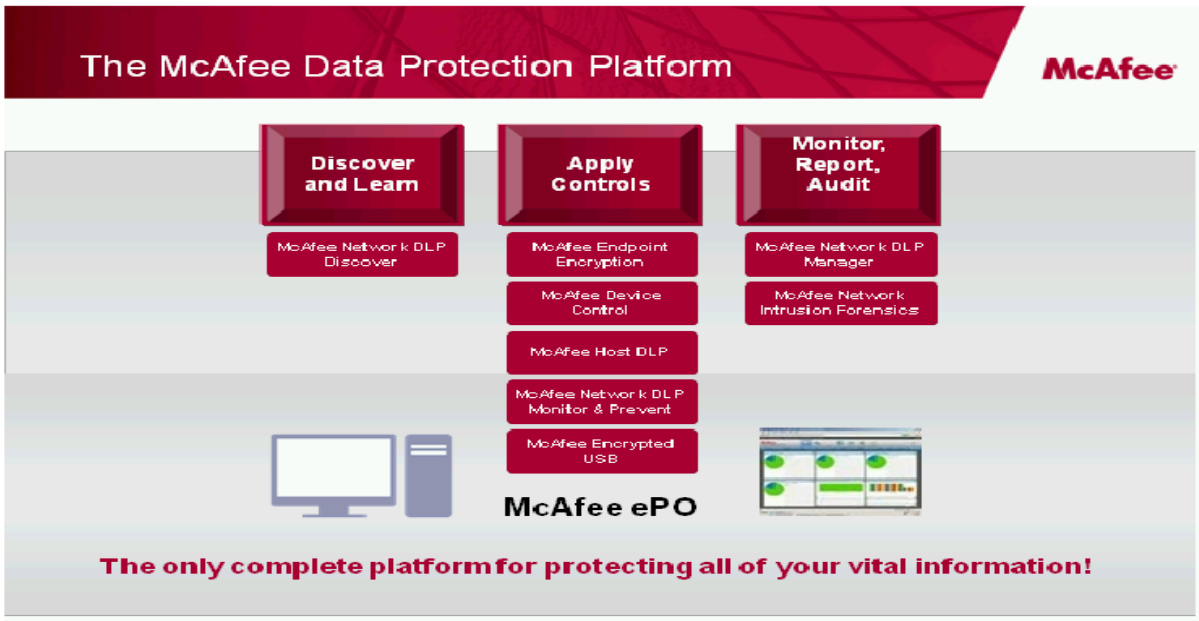


Figure 7 : Plateforme de McAfee DLP

7. Conclusion

Les solutions DLP sont multiple a savoir CA DLP, McAfee DLP, EMC/RSA (Tablus), Symantec (Vontu), Vericept, chacune a ses propres caractéristiques afin d'identifie, surveille et protège les données la ou sont stockées, en cours d'utilisation ou en mouvement quel que soit le support.

Il existe également d'autre solutions que ca soit des solutions intégrés partielles (Code Green Networks, GTB Technologies, Trend Micro (Provilla),), ainsi des solutions purement réseaux (Clearswift, Fidelis Security Systems, Palisade Systems, Proofpoint) et des solutions uniquement terminaux (NextSentry , Verdasys, Utimaco). Donc il y a plusieurs solutions DLP, il suffit de bien savoir ce que veut l'entreprise et de disposer de tout le soutien patronal nécessaire.

Chapitre III : Etude comparative

Au cours de ces dernières années, quelques domaines technologiques en matière de sécurité et de gestion des risques ont vu des niveaux similaires d'attention et d'activité que la prévention des fuites de données (DLP). C'est parce que DLP a un enjeu fort dans pratiquement toutes les tendances actuelles en matière de sécurité et la gestion des risques.
Alors que les entreprises se rendent compte qu'ils ont besoin de protéger leurs actifs informationnels au lieu de continue de les protégées par les anciens méthodes. Viens le Chiffrement, sécurité des terminaux et, surtout, des solutions DLP promesse pour les aident à protégé leur biens électroniques.
En fin de compte, ces technologies découvrir, comprendre, gérer et protéger les informations, ils sont donc un rôle essentiel dans toute stratégie moderne de sécurité et de gestion des risques.
À l'origine, les organismes se sont tournés vers la DLP parce qu'ils ont été forcés par les règlements externes ou parce qu'ils ont voulu protéger des données sensibles de quitter l'entreprise via les différents canaux de communication. Les risques ont évolué, ainsi que le marché du DLP.

1. Le Choix de la solution

Pour réussir l'objectif de protection des données sensibles, les solutions DLP doivent accomplir 5 Missions principales :

- Découvrir :

Les moteurs de DLP identifient et localisent automatiquement toutes les données existantes au sein d'un écosystème informatique (des systèmes de stockage aux périphériques, des serveurs aux réseaux). Cette action de découverte permet de réaliser une cartographie exhaustive de l'implantation des données et des flux d'information entre systèmes et entre utilisateurs.

- Classifier :

Après la découverte, la classification permet d'attribuer à chaque donnée un niveau de criticité qui déterminera l'étendue des mesures de contrôle et de sécurité auxquelles la donnée sera soumise. L'approche DLP permet d'appliquer de manière automatique la politique de classification à toutes les données découvertes et le niveau de criticité associé à chaque donnée régira alors l'usage et la circulation de cette dernière sur l'ensemble de l'écosystème informatique. Cette classification n'est pas le fait de l'utilisateur, elle est appliquée automatiquement aux données par la solution de DLP. Par exemple un fichier contenant des numéros de cartes bancaires sera classé comme « très sensible » vis-à-vis d'une politique comme PCI/DSS, et cette classification sera utilisée par le gestionnaire pour déclencher les actions de protection.

- Gérer :

La gestion centralisée de la politique est un point central du DLP. Les outils de cette gestion centralisée permettent une vision exhaustive et un contrôle très fin des données classées qu'elles soient au repos, en cours d'utilisation ou en transit sur le réseau. Dès qu'une donnée est manipulée, son niveau de criticité (attribué lors de la classification) détermine l'application automatique des consignes de sécurité associées et répertorie toutes les opérations effectuées sur ces données.

- Appliquer :

Cette étape concerne l'exécution effective des contrôles de sécurité, lorsque les données classées sont manipulées, conformément aux politiques internes et réglementaires de gestion du risque. Par exemple, les contrôles appliqués aux données au repos dans un data center peuvent inclure la mise en quarantaine, le déplacement, c'est-à-dire des contrôles associés par un utilisateur à un fichier autorisant ou empêchant la lecture/la copie/ l'impression, etc. Pour les données en transit sur le réseau, les contrôles incluent le blocage, le chiffrement, etc., tandis que les contrôles sur les données en cours d'utilisation sur un poste de travail peuvent inclure le blocage de l'action, une demande de justification de l'action, ou tout simplement l'audit.

- Signalement et rapports :

Cette action fait partie de la logique globale du contrôle élargi des flux de données. Les infractions à la politique de sécurité peuvent être signalées à l'utilisateur au management, au responsable de la sécurité, au service informatique ou à la division de conformité juridique. Utilisé principalement à des fins éducatives, le signalement peut également être utilisé pour recueillir des traces ou preuves (par exemple les données contextuelles de l'infraction de sécurité telles que l'identité, les scénarios de connexion, le moment et le lieu où l'événement s'est produit). A ce niveau une interaction avec une solution SIEM permet d'avoir une vue unique et haut niveau sur les incidents de sécurité et de gestion. Cette interaction entre DLP et SIEM facilite la corrélation en temps réel des événements de sécurité du système de données et accélère la réponse pour remédier à toute fuite de données.

2. Etude comparative

Par la suite je vais vous présenté une étude comparative entre les différents solutions DLP existant dans le marché, je me suis basé sur deux études, celle de Forrester «**The_Forrester_Wave_DataLeakPrevention_Q2_2008** » en juin 2008 et une autre de Gartner « **Magic Quadrant for Content-Aware Data Loss Prevention**» en 22 Juin 2009.

- Etude FORRESTER

Forrester Research, Inc est une société de recherche indépendante qui fournit des conseils pragmatiques aux chefs mondiaux en gestion des affaires et de la technologie. Depuis plus de 25 ans, Forrester a été prise de IT, le marketing et l'industrie de technologie les leaders de réussite.

D'après Forrester les critères de comparaison qui sont regroupés dans trois niveaux:

- l'offre actuelle

Avec la sélection de domaines clés de la fonctionnalité du produit: les données en mouvement (réseau), des données au repos, des données en cours d'utilisation (ordinateur de bureau), gestion de la politique et l'intégration.

- Stratégie

Afin d'évaluer la stratégie globale de chaque fournisseur, elle a choisi des critères basés sur la vision de l'entreprise et sa stratégie de produit et le prix.

- Présence dans le marché

Dans cette étude Forrester est focalisé sur 11 fournisseurs à savoir Code Green Networks, InfoWatch, McAfee, Orchestria, Reconnex, RSA Security, Trend Micro, Verdasys, Vericept, Websense, et Workshare.

2.1 Comparaison

D'après cette étude les solutions sont classées en 4 catégories :

- leaders

Websense intégré avec succès Port Authority dans son portefeuille de sécurité de contenu et offre une forte stratégie. Reconnex offre les meilleures fonctionnalités du produit de sa catégorie grâce à son classement automatisé et un moteur d'analyse, qui permet aux clients de reposer sur les données réelles et que le moteur de contrôle pour savoir ce qui est important a protéger. Verdasys leader capacités DIU (Data in use) et offre une analyse riche basée sur le contexte et la détection dans tous les données. RSA Security la meilleure vision intégrée de la DLP et offre des capacités de découverte exceptionnelle qu'elle a acquis de Tablus.

Vericept offre un produit DIM (Data in motion) avec DIU (Data in use) et des capacités solides DAR (Data at rest) et le leader de marché des capacités de gestion des politiques. Pendant ce temps, Symantec (par l'acquisition de Vontu) offre une plateforme DLP avec des capacités équilibrées pour DIM (Data in motion) et DAR (Data at rest), et il détient le potentiel pour fournir une intégration profonde dans la sécurité, le stockage et la gestion de l'information.

- Performance

Workshare propose une stratégie équilibrée et une intégration étroite dans Microsot Office. Il est également le seul fournisseur qui peut nettoyer les métadonnées dans les documents. Orchestria expose de haute précision, facilité de déploiement, et de grande administration et de reporting.

Code Green Networks fournit une solution solide, facile à mettre en œuvre avec l'utilisation des appareils DLP qui sont très rentable.

McAfee et Trend Micro cherchent à étendre leurs offres de sécurité au sens large avec de solides capacités de protection des données. Bien que les deux commencent à partir de l'extrémité, McAfee intègre le chiffrement (SafeBoot) et la gestion ePolicy, tandis que les moules Trend Micro le Provilla DIU (Data in use) produit dans sa suite de sécurité.

InfoWatch est un concurrent, offre des services spécialisés valeur pour les clients en Russie et en Europe de l'Est. Le produit offre une bonne administration et de solides capacités de DIM (Data in motion), mais manque dans de nombreuses autres fonctionnalités.

La figure suivant représente classification des solutions DLP basé sur 74 critères.

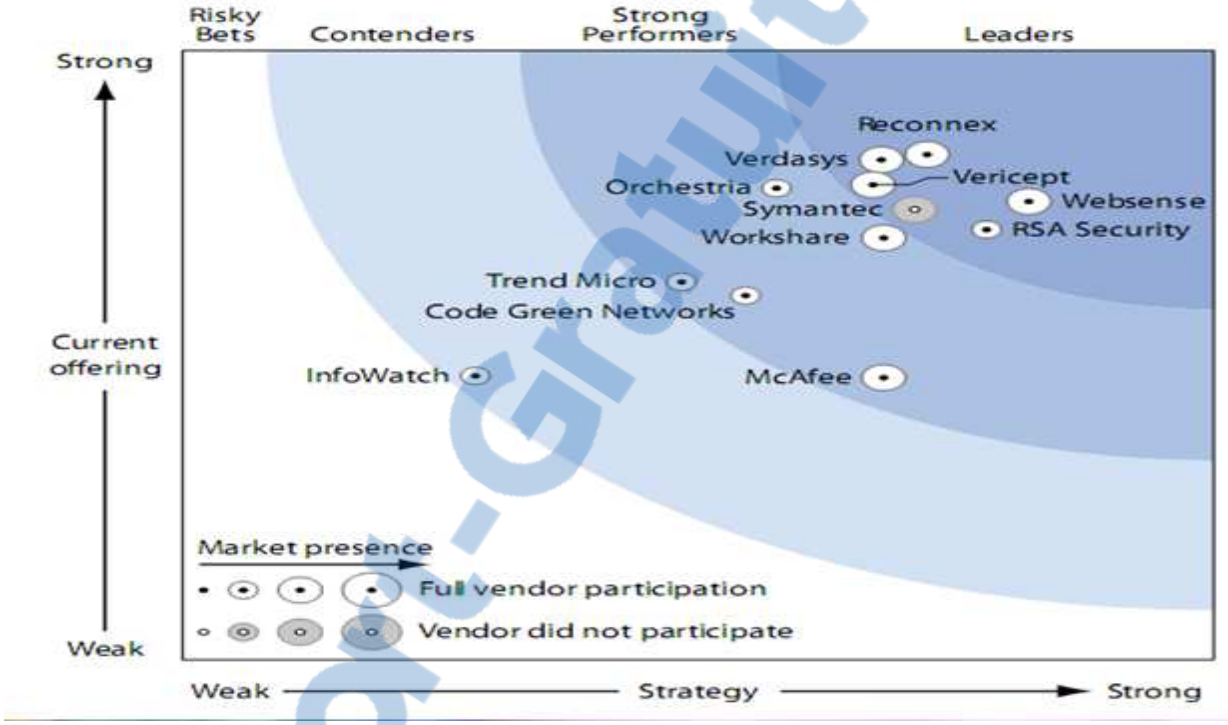


Figure : 8 The_Forrester_Wave_DataLeakPrevention_Q2_2008

	Forrester's Weighting	Code Green Networks	InfoWatch	McAfee	Orchestria	Reconnex	RSA Security	Trend Micro	Verdasys	Vericept	Websense	Workshare
CURRENT OFFERING	50%	2.99	2.33	2.31	3.87	4.14	3.53	3.10	4.10	3.90	3.76	3.46
Solution breadth and technology	15%	3.70	2.60	3.70	2.55	3.15	3.00	3.50	4.50	3.40	3.30	3.45
Data-in-motion (i.e., the network piece)	10%	4.60	3.00	3.00	4.20	5.00	4.20	2.60	3.40	5.00	5.00	3.80
Data-at-rest (i.e., discovery)	12%	2.20	2.20	0.40	3.80	4.60	4.60	3.40	4.20	4.60	4.20	2.60
Data-in-use (i.e., desktop or host)	13%	3.00	1.80	2.60	4.20	3.80	2.60	4.20	5.00	3.40	3.00	3.40
Unified management	5%	0.00	2.40	1.00	5.00	5.00	0.30	4.40	5.00	4.40	4.40	4.40
Policy management	5%	3.20	2.60	1.80	3.80	4.20	4.00	2.40	4.20	4.60	4.20	2.80
Administration	5%	3.00	5.00	1.00	5.00	5.00	5.00	3.00	5.00	5.00	3.00	5.00
Forensics	10%	2.40	2.00	3.00	3.80	4.60	3.40	2.20	4.60	4.20	3.40	4.20
Integration	10%	2.00	1.60	0.80	2.90	3.70	2.90	1.70	2.50	3.10	4.40	3.30
Customer references	15%	3.80	1.90	3.30	4.70	3.90	4.50	3.20	3.40	3.10	3.40	3.00
STRATEGY	50%	2.73	1.42	3.40	2.88	3.61	3.90	2.42	3.39	3.35	4.10	3.40
Company vision and product strategy	70%	2.80	1.30	2.80	3.00	4.10	4.60	2.60	3.70	3.60	4.10	2.80
Go-to-market	30%	2.55	1.70	4.80	2.60	2.45	2.25	2.00	2.65	2.75	4.10	4.80
Pricing and cost	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
MARKET PRESENCE	0%	2.85	2.35	3.38	2.70	3.30	2.58	2.40	3.75	3.38	3.60	3.08
Installed base	50%	2.90	1.80	4.50	1.50	2.90	1.80	2.10	3.60	4.20	4.50	4.70
Revenue	50%	2.80	2.90	2.25	3.90	3.70	3.35	2.70	3.90	2.55	2.70	1.45

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

Figure 9 : suite de The_Forrester_Wave_DataLeakPrevention_Q2_2008

Donc Forrester a évalué de principaux fournisseurs DLP de données à travers approximativement 74 critères, elle a constaté que Websense et Reconnex se sont trouvés en première position en raison de leur forte stratégie du marché. Verdasys est un leader dû à la fonctionnalité équilibrée et à l'analyse basée sur contexte riche au Desktop. RSA Security se distingue par sa vision intégrée et les capacités de découverte de premier plan, tandis que Vericept complète la tête de la catégorie de l'année 2008 en raison de sa couverture DLP très équilibré et d'analyse solides. Code Green Networks est facile à utiliser, rentable, et un ajustement idéal pour les petites et moyennes entreprises (PME).McAfee propose désormais une forte intégration avec le cryptage ; Trend Micro leader international fort en matière de protection des données en utilisation. Basé en Russie InfoWatch est un concurrent et offre une solution simple DLP pour de nombreuses organisations en Europe orientale et au Moyen-Orient. En fin de compte, DLP sera une nécessité qui est intégré à l'infrastructure de sécurité; à plus long terme, il s'étendra à la gestion de l'information.

- **Etude Gartner**

Gartner, Inc., fondée en 1979, est une entreprise américaine de conseil et de recherche dans le domaine des techniques avancées. Ayant environ 10 000 clients, elle mène des recherches, fournit des services de consultation, tient à jour différentes statistiques et maintient un service de nouvelles spécialisées.

Gartner utilise le terme «contenu-Aware DLP» pour décrire un ensemble de technologies et de techniques d'inspection utilisées pour classer le contenu des informations contenues dans un objet (par exemple, un fichier, un message e-mail, un paquet, une application ou un ensemble de données de stockage, au cours d'utilisation ou en mouvement à travers un réseau).

Il décrit également la capacité d'appliquer une politique dynamique (par exemple, par l'exploitation de rapports, de classement, le déplacement, le marquage, le cryptage).

Les fournisseurs ont été inclus dans ce «Magic Quadrant» si leurs offres:

• Détecter les opérations de contenu sensible de toute combinaison de trafic réseau, les données au repos ou point de terminaison.

• Peut détecter les contenus sensibles en utilisant des techniques sophistiquées de détection sensibles au contenu, y compris les correspondants document partiel , la structure de données des empreintes digitales, analyse statistique, correspondant à l'expression régulière, des analyses conceptuelles et lexique, et les mots clés.

•Prennent en charge la détection de contenu des données sensibles dans des données structurées et non structurées.

• Peut bloquer, au minimum, la politique de violations qui se produisent sur les communications par e-mail.

• sont généralement disponibles à partir de 31December2008

• sont déployées dans des environnements de production des clients, avec au moins cinq références.

Les fournisseurs ont été exclus de cette «Magic Quadrant» si leurs offres:

• Utiliser des mécanismes simples de détection de données (par exemple, l'appui seulement ciblage des mots clés, lexique,ou de simples expressions régulières)

• Ont des fonctions réseau qui supporte moins de quatre protocoles (par exemple, e-mail, messagerie instantanée et HTTP).

La figure suivant présente les résultats de cette études, qui repartie les produits en 4 catégories.

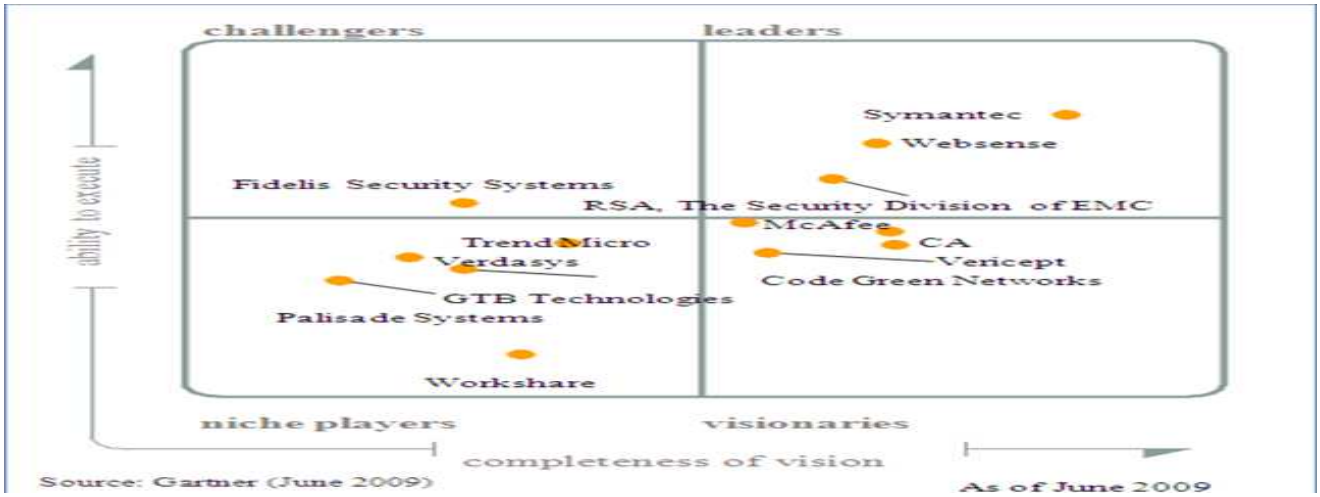


Figure 10 : Magic Quadrant for Content-Aware Data Loss Prevention

- Leaders

Les Leaders sont seulement trois fournisseurs pour l'année 2009, parce que ce marché continue d'évoluer. Ils ont fait preuve d'une bonne compréhension des besoins des clients et offrent des capacités complètes dans les trois domaines fonctionnels soit réseau, la découverte et point de terminaison, ainsi grâce à des partenariats bien établis et une intégration étroite. Ce qui leurs permet d'intégrer pleinement des fonctionnalités améliorées en cours de développement et de répondre à l'évolution des besoins du marché. Les leaders sont les suivants:

• RSA,TheSecurity Division of EMC
• Symantec
• Websense

- Challengers

Les systèmes de sécurité de Fidelis sont dans le quart de cercle de challengeurs - le seul Fidelis Security Systems se trouve dans le quadrant des challengers, le seul fournisseur qui a obtenu ce statut pour 2009 fondée sur l'exécution et le succès en tant que fournisseur a canal unique DLP Gartner estime que Fidelis peu probable que jamais pour devenir parmi les leaders DLP.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

- visionnaires

Les quatre fournisseurs dans le quadrant des visionnaires ont des origines très différentes sur ce marché. CA, à la suite de son acquisition d'Orchestria, a une bonne vision et le potentiel d'augmenter dans le «Leaders Quadrant» de l'année prochaine avec une solide exécution sur sa feuille de route et les ventes. Code Green Networks, qui a une offre de qualité pour les petites et moyennes entreprises (PME), a publié une version entreprise, mais n'a pas un historique de succès avec les grandes entreprises. McAfee acquis Reconnex, qui était dans le «Leaders Quadrant» en 2008, McAfee comme un visionnaire pour 2009, mais avec quelques exécution efficace de son feuille de route, la société devrait être de retour dans le «Leaders Quadrant» en 2010. Vericept, l'un des rares fournisseurs indépendants sur ce marché, a connu des difficultés d'exécution et a donc été rétrogradé de leader au visionnaire.

- Niche Players

Le quadrant Niche Players a cinq fournisseurs pour 2009. GTB et les systèmes de palissade sont de petits démarrages qui continuent à jouer le « rattrapage».Trend Micro a montré une certaine innovation, mais n'a pas encore publiquement articuler une vision globale de son approche de la DLP. Verdasys a été un challenger l'année dernière, mais a souffert d'un manque de concentration et de la visibilité sur ce marché. Workshare a des caractéristiques de compétition, mais n'a pas été en mesure d'exécuter en termes de ventes ou de déploiements pour les fonctions sensibles au contenu

3. Conclusion

Donc le marché de DLP continue de progresser, Là plupart des activités de marché dans la dernière année a été focalisé sur de surveillance réseau multicanaux, mais la vue de Gartner est d'intégrées le contrôle réseau et les points de terminaison comme le but ultime de la destination finale du marché. Les entreprises devraient utiliser Technologies DLP pour élaborer et appliquer de meilleures pratiques commerciales dans le traitement et la transmission de données sensibles et les vendeurs doivent reconnaître que c'est là que réside la valeur de leurs produits. DLP repose essentiellement sur la gestion des risques et la politique de sécurité appliquée aux données sensibles, la recherche de données, et le contrôle de son utilisation.

Chapitre IV : Focus sur McAfee Host Data Loss Prevention

Le logiciel McAfee Host Data Loss Prevention protège les entreprises contre les risques associés aux transferts non autorisés de données, à l'intérieur ou à l'extérieur de l'entreprise. L'expression « fuite de données » implique la diffusion au-delà des frontières de l'entreprise d'informations de nature confidentielle ou privée, à la suite d'une communication non autorisée via divers canaux de transfert, notamment des applications, des périphériques physiques ou des protocoles réseau.

1. Qu'est-ce que McAfee Host Data Loss Prevention ?

Le logiciel McAfee Host Data Loss Prevention est une solution qui a recours à des agents pour surveiller et contrôler les actions des utilisateurs de l'entreprise en rapport avec du contenu sensible, dans leur propre environnement de travail, à savoir leurs ordinateurs. Elle utilise une technologie avancée de détection et des dictionnaires prédéfinis pour identifier ce contenu et intègre la gestion et le chiffrement des périphériques pour des niveaux de contrôle supplémentaires.

Le logiciel McAfee Host Data Loss Prevention présente les caractéristiques suivantes :

• **Protection universelle** : assure une protection contre les fuites de données par le contrôle du plus large éventail de canaux de transmission d'informations.

• **Protection des données en fonction du contenu** : protège contre les fuites de données, quel que soit le format dans lequel les données sont enregistrées ou manipulées sans pour autant perturber les activités légitimes de l'utilisateur.

•**Protection nomade** : bloque la transmission des données sensibles depuis les postes de travail et les ordinateurs portables, qu'ils soient ou non connectés au réseau de l'entreprise.

2. Présentation des composants et interactions

Le logiciel McAfee Host Data Loss Prevention est constitué de plusieurs composants. Chacun de ces composants joue un rôle précis dans la protection de réseau contre les fuites de données.

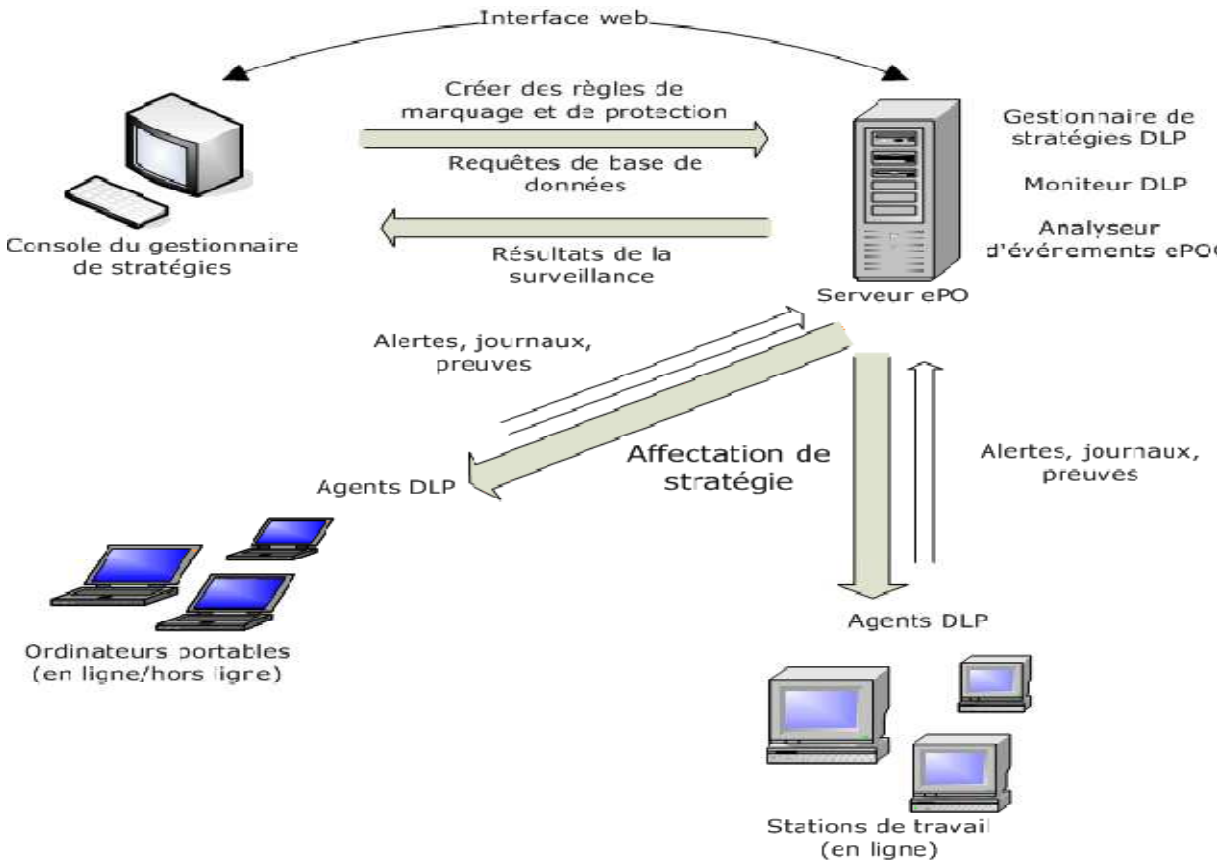


Figure 11 : McAfee Host Data Loss Prevention

Ces composants sont les suivants :

- **Console du gestionnaire de stratégies Host DLP**

La console du gestionnaire de stratégies Host DLP est l'interface au sein de laquelle l'administrateur définit et met en œuvre la stratégie de sécurité pour les informations de l'entreprise. Il permet de créer la stratégie de sécurité des informations et d'administrer les composants de McAfee Host Data Loss Prevention.

- **Agent DLP**

Les agents DLP sont installés sur les ordinateurs de l'entreprise, également appelés ordinateurs gérés ; ils mettent en œuvre les stratégies définies dans le gestionnaire de stratégies Host DLP. Les agents contrôlent les activités des utilisateurs ; ils effectuent des opérations de surveillance et de vérification et préviennent toute copie ou tout transfert de données sensibles par des utilisateurs non autorisés. Ils génèrent également des événements enregistrés par l'analyseur d'événements ePO.

- **Analyseur d'événements ePO**

Les événements générés par les agents DLP sont envoyés à l'analyseur d'événements ePO et enregistrés dans des tables de la base de données ePO. Ils sont stockés dans la base de données en vue d'analyses complémentaires et utilisés par d'autres composants du système.

- **Moniteur Host DLP**

Les événements envoyés à l'analyseur d'événements DLP sont affichés dans le moniteur Host DLP, interface accessible via la console de génération de rapports d'ePolicy Orchestrator. Tous les événements peuvent être filtrés et triés en fonction de différents critères, tels que les règles de protection, la gravité, la date, l'heure, l'utilisateur, le nom de l'ordinateur ou la version de la stratégie.

3. Fonctionnement de McAfee Data Loss Prevention

McAfee Host Data Loss Prevention protège les informations sensibles de l'entreprise grâce au déploiement de stratégies contenant des règles de classification, des règles de marquage, des règles de protection, ainsi que des affectations d'utilisateurs et de groupes. Les stratégies sont surveillées et les actions définies sont surveillées ou bloquées si nécessaire. Les contenus pertinents sont enregistrés en tant que preuves et des rapports sont générés en vue de l'examen et du contrôle du processus.

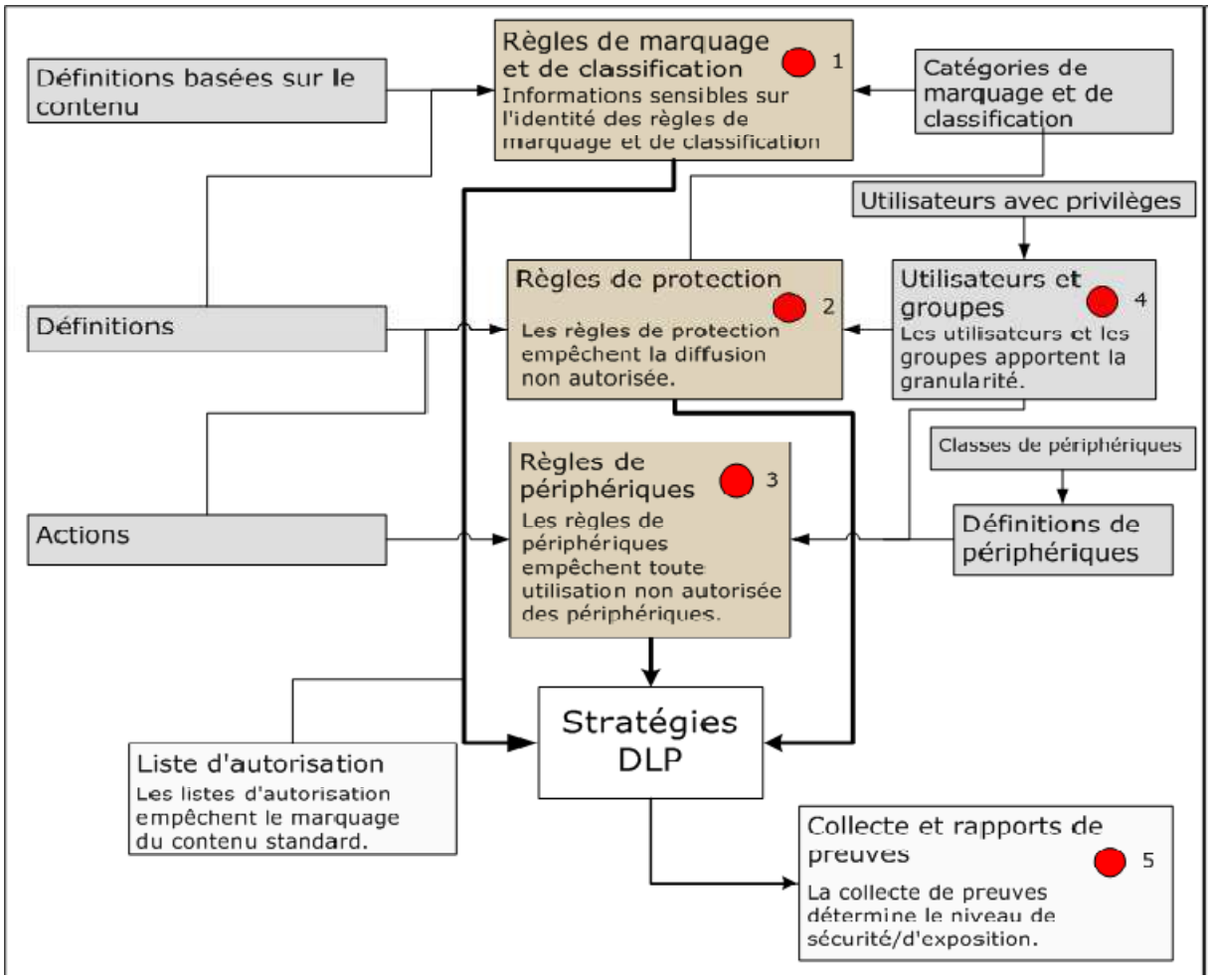


Figure 12 : Flux de travail McAfee Host Data Loss Prevention

- **Règles de marquage et de classification**

Les règles de marquage et de classification, définies selon les besoins de l'entreprise, identifient les informations confidentielles et leurs sources. Les données peuvent être classées selon divers critères :

• **Application** : les règles de marquage peuvent appliquer des marqueurs de façon générique, en fonction des applications à l'origine de la création d'un fichier ou encore du type de fichier ou de son extension.

• **Contenu** : les catégories de contenu sont appliquées en fonction de l'analyse syntaxique du contenu et des résultats de sa comparaison avec des mots-clés ou des modèles prédéfinis.
Il existe deux types de règles de classification :

• Règles de classification en fonction du contenu : permettent de comparer le contenu à des chaînes prédéfinies et à des modèles textuels ou à des dictionnaires.

• Règles de classification des documents enregistrés : permettent de classifier l'ensemble du contenu spécifié dans un groupe de dossiers défini.

• **Emplacement** : lorsque des fichiers sont copiés ou que des processus locaux y accèdent, des marqueurs sont appliqués en fonction de l'emplacement du fichier source. A titre d'exemple, un fichier copié en local à partir d'un partage sur un serveur réseau.

- **Règles de protection**

Les règles de protection permettent de bloquer la distribution non autorisée des données marquées. Lorsqu'un utilisateur tente de copier des données marquées ou de les joindre à un e-mail, les règles de protection déterminent si cette opération doit être autorisée, surveillée ou bloquée. Les règles de protection sont définies avec des applications ou des groupes, des affectations d'utilisateurs ou des définitions telles que les destinations e-mail ou les modèles textuels.

- **Règles de périphériques**

Les règles de périphériques surveillent le système et l'empêchent éventuellement de charger des périphériques physiques, notamment des périphériques de stockage amovibles, Bluetooth, Wi-Fi et autres périphériques Plug-and-Play. Les classes et les définitions de périphériques permettent de définir des règles de périphériques. Les règles de périphériques de stockage amovibles proposent des options supplémentaires qui permettent de configurer le périphérique en lecture seule et de bloquer l'écriture de données.

- **Règles de découverte**

DLP Discovery est un robot qui s'exécute sur les machines clientes. Les règles de découverte définissent le contenu recherché et si celui-ci doit être surveillé, mis en quarantaine, chiffré ou supprimé. Les paramètres de la configuration globale des agents déterminent quand et où la recherche est effectuée.

- **Groupes d'affectation**

Les groupes d'affectation appliquent des règles de protection spécifiques à différents groupes, utilisateurs et ordinateurs de l'entreprise.

- **Stratégies et déploiement de stratégies**

Une stratégie est une combinaison de règles de marquage, de règles de protection, de définitions et de groupes d'affectation. Les stratégies sont déployées par ePolicy Orchestrator sur les ordinateurs gérés de l'entreprise (ordinateurs sur lesquels un agent DLP est installé).

- **Surveillance**

• **Surveillance des événements** : le moniteur Host DLP permet aux administrateurs de consulter les événements des agents au fur et à mesure de leur réception.

• **Collecte de preuves** : si des règles de protection sont définies pour collecter des preuves, une copie des données marquées est sauvegardée et liée à l'événement spécifique. Ces informations permettent de déterminer la gravité ou l'exposition en termes de risque de l'événement. Les preuves sont chiffrées à l'aide de l'algorithme AES avant d'être enregistrées.

- **Listes d'autorisation**

Les listes d'autorisation sont des ensembles d'événements que le système doit ignorer. Le dossier de liste d'autorisation contient des fichiers texte qui définissent le contenu (généralement passe-partout) non marqué, ni restreint. L'objectif principal de ce système consiste à améliorer l'efficacité du processus de marquage en ignorant le contenu standard qui n'a pas besoin d'être protégé.

4. Chiffrement

Le chiffrement de documents critiques joue un rôle important dans une stratégie de sécurité solide. Le logiciel McAfee Host Data Loss Prevention prend en charge le chiffrement de plusieurs manières :

• Définitions de périphériques intégrées pour identifier les périphériques McAfee Encrypted USB (anciennement SafeBoot DE) et le contenu chiffré à l'aide de McAfee Endpoint Encryption (anciennement SafeBoot CE).

• Règles de filtrage selon les propriétés des documents (chiffré/non chiffré).

• Chiffrement à la demande.

• Définitions de clés de chiffrement.

5. Console du gestionnaire de stratégies Host DLP

La console du gestionnaire de stratégies Host DLP constitue l'interface du logiciel McAfee Host Data Loss Prevention. Cette interface permet de créer et de mettre en œuvre des stratégies chargées de protéger les informations sensibles de l'entreprise. A cet emplacement, l'administrateur peut créer, modifier et contrôler les objets et les règles système destinés à prévenir les fuites de donnée

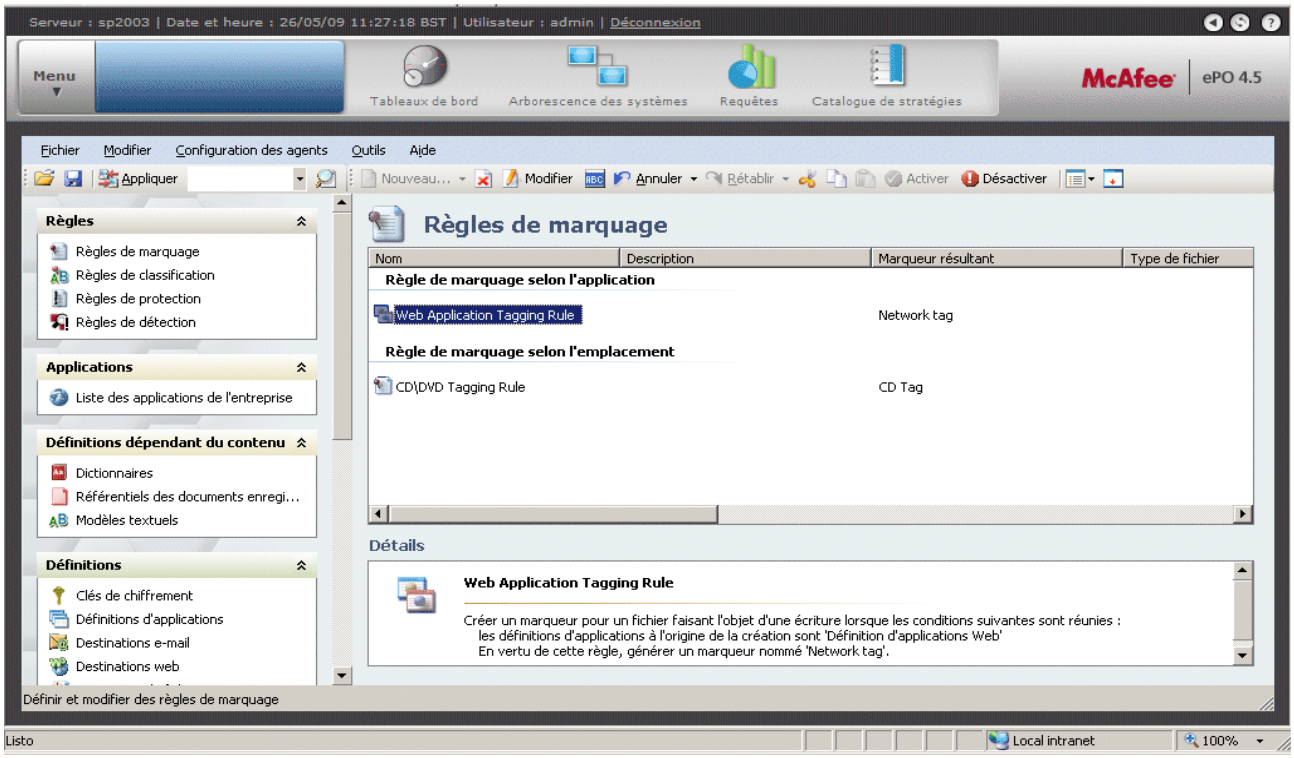


Figure 13 : Gestionnaire de stratégies Host DLP dans la console ePolicy Orchestrator 4.5

Le gestionnaire de stratégies Host DLP comporte plusieurs sections :

- **Barre de navigation** :

Une zone dans laquelle l'administrateur sélectionne une règle ou une définition.

• **Règles** : les Règles de marquage ou Règles de classification pour classifier le contenu, Règles de protection pour mettre en œuvre les stratégies définies et Règles de découverte pour rechercher du contenu sensible dans votre réseau.

• **Applications** : Liste des applications.

• **Définitions dépendant du contenu** et **Définitions** : permet de créer de nouveaux objets pour les règles du système.

• **Gestion des périphériques** : permet de surveiller et de contrôler l'utilisation des périphériques physiques.

• **Affectation de stratégie** : permet de créer et de gérer des groupes d'utilisateurs pour le déploiement des stratégies, ainsi que des groupes d'utilisateurs avec privilèges qui prévalent sur les stratégies mises en œuvre.

• **Administration de la base de données** : permet de surveiller et de gérer la base de données du système.

- **Panneau principal** : permet à l'administrateur système de modifier et de revoir des règles ou des définitions, en fonction de l'objet sélectionné dans la barre de navigation.

- **Volet de détails** : affiche une description détaillée d'un objet unique sélectionné dans le panneau principal.

6. Quelle Démarche Adopter ?

La mise en œuvre du DLP est un processus itératif en 3 étapes:

➢ Étape 1 :

Découvrir et évaluer les informations, structurées ou non, quelle qu'en soit la Localisation dans l'infrastructure informatique, et l'état (en cours d'utilisation sur un poste, en transit sur le réseau ou au repos dans un data center).

➢ Étape 2 :

Créer des politiques pour détecter et protéger les informations qu'elles soient en cours d'utilisation, au repos ou en transit. Démarrer par exemple avec des modèles qui appliquent systématiquement la plupart des réglementations.

➢ Étape 3 :

Appliquer les politiques aux divers référentiels de stockage, aux passerelles réseau, aux postes et périphériques utilisateurs, en ligne et hors ligne, afin d'identifier toute violation de politique et prendre en temps réel des mesures correctives ou d'alertes pour empêcher que les données sortent de l'organisation par inadvertance

7. Conclusion

Les outils de DLP (Data Loss Prevention) visent à empêcher la fuite d'informations sensibles.
Ils tissent une toile qui surveille le réseau, le stockage, les serveurs et les PC.. Le nombre d'incidents signalés liés à la fuite de données est en hausse. Il est impératif que les entreprises disposent d'une visibilité et d'un contrôle permanents sur les transferts de leurs données confidentielles. Grâce à ses fonctions de surveillance en temps réel du trafic, la solution McAfee Host Data Loss Prevention permet de prévenir les fuites de données sur le lieu de travail, au domicile et en déplacement. Cette solution complète basée sur l'hôte protège les entreprises contre les risques de pertes financières, de préjudice porté à sa marque et de non-conformité.

Rapport-Gratuit.com

Chapitre V : Réalisation de la maquette de test

Maintenant qu'on a fait connaissance de la solution McAfee Host Data loss prevention, on passe à la phase de la mise en œuvre d'une maquette de test de la solution HDLP. Afin de vérifier ses différents fonctions à savoir : la surveillance instantanée et aisée des événements en temps réel, application de stratégies de sécurité gérées de façon centralisée afin de réglementer, voire de restreindre, l'utilisation et les transferts de données sensibles par le personnel, ou encore génération de rapports détaillés. Le tout sans perturber les activités des entreprises. Egalement les Protéger contre les vecteurs de fuite internes, comme la messagerie électronique ou instantanée, la gravure de CD, la publication web, la copie sur périphériques USB et l'impression.

1. Architecture de la maquette

Cette maquette de test est qui composé d'un serveur et un poste de travail virtuel dans le même réseau à l'aide de l'outil de virtualisation VMware version 6.

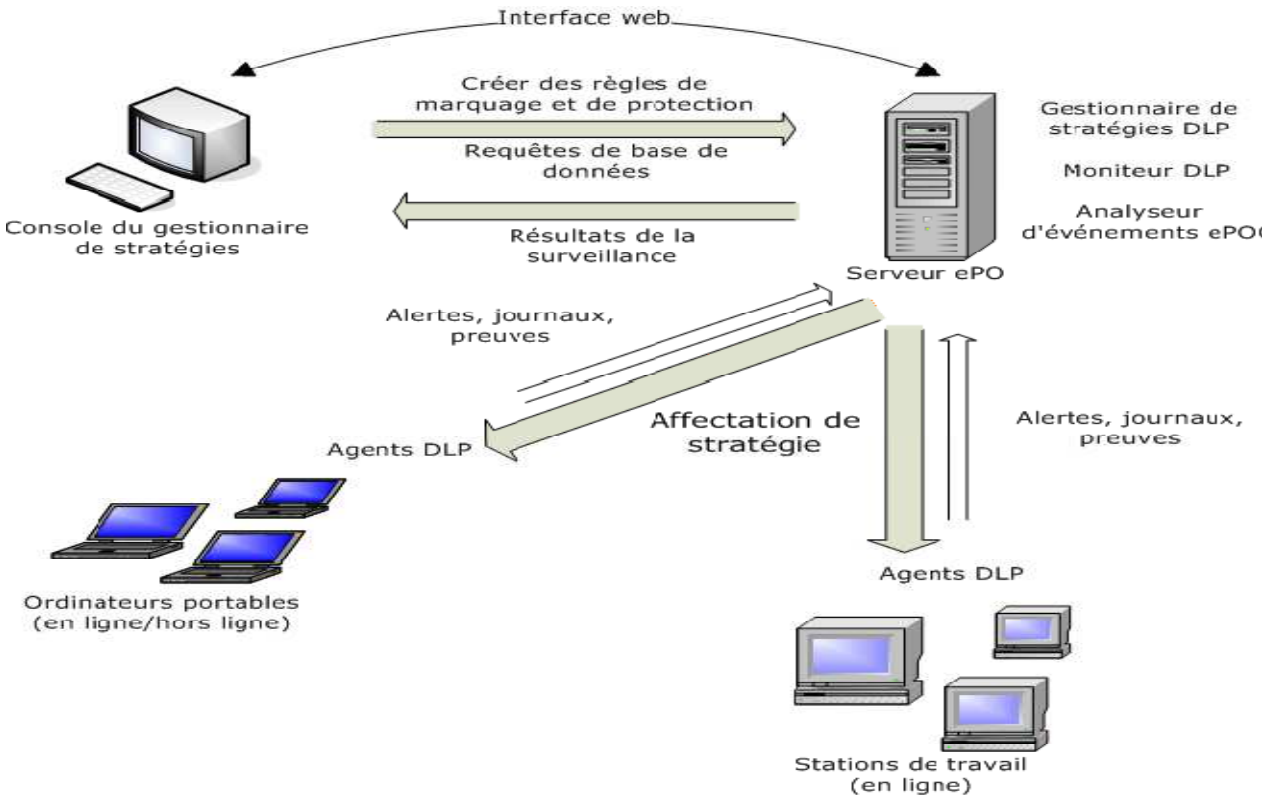


Figure 13 : Architecture de maquette de test

2. Installation et configuration de McAfee Host Data Loss Prevention

Dans cette partie on se concentré sur les informations nécessaires à l'installation du logiciel McAfee Host Data Loss Prevention version 9.0. Le détail les différentes étapes de l'installation, ainsi que les vérifications à effectuées.

2.1 Avant l'installation

- **Configuration du système**

a. Matériels requise

Il est recommandé d'utiliser le matériel suivant pour exécuter et assurer le bon fonctionnement de logiciel McAfee Host Data Loss Prevention version 9.0 :

Type de matériel	Caractéristiques techniques
Serveur	• **Processeur** : Intel Pentium IV 2,8 GHz ou plus. • **Mémoire vive (RAM)** : • 512 Mo au minimum pour McAfee Device Control uniquement (1 Go recommandé). • 1 Go au minimum pour l'ensemble de McAfee Host Data Loss Prevention (2 Go recommandés). • **Disque dur** : 80 Go au minimum.
Poste de travail agent	• **Processeur** : Pentium III 1 GHz ou plus. • **Mémoire vive (RAM)** : • 512 Mo au minimum pour l'ensemble de McAfee Host Data Loss Prevention (1 Go recommandé). • **Disque dur** : 200 Mo au minimum.
Réseau	Réseau LAN de 100 Mbits desservant tous les postes de travail et le serveur ePO.

Tableau 1 : Matériels requise pour installation de HDLP

Les systèmes d'exploitation pris en charge sont les suivants :

Type d'ordinateur	Logiciels
Serveur	• Windows 2003 Server Standard Edition (SE) Service Pack 1 ou ultérieur • Windows 2003 Enterprise Edition (EE) Service Pack 1 ou ultérieur
Poste de travail de l'agent	• Windows 2000 Professionnel SP4 ou ultérieur 32 bits • Windows XP Professionnel Service Pack 1 ou ultérieur (32 bits uniquement) • Windows Vista ou Service Pack 1 (32 bits uniquement)

Tableau 2 : Les systèmes d'exploitation pris en charge pour installation de HDLP

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

Noté bien que l'utilisateur qui installe le logiciel McAfee Host Data Loss Prevention version 9.0 sur les serveurs doit être membre du groupe des administrateurs locaux.

b. Logiciels serveur

Le logiciel suivant est nécessaire sur le serveur exécutant le moniteur et le gestionnaire de stratégies Host DLP :

Logiciel	Version
McAfee ePolicy Orchestrator	4.0 Patch 4 ou ultérieur 4.5
McAfee Agent	4.0 Patch 1 ou ultérieur
McAfee Système d'aide ePolicy Orchestrator	• pour ePO 4.0, téléchargez le package de l'aide ePO complet le plus récent contenant l'aide Help HDLP 9.0 • pour ePO 4.5, téléchargez l'extension Help HDLP 9.0.
Microsoft .NET	3.5 (Patch 1 recommandé)
Microsoft SQL Server	2005 ou ultérieur

Tableau 3 : Logiciel nécessaire sur le serveur

- **Configuration du serveur**

Avant de procéder à l'installation on doit s'assurer que le serveur présent bien la configuration système minimum requise. On effectue les taches suivantes :

- Installation Microsoft Windows 2003 Standard Edition Service Pack 1 avec le rôle de serveur de fichiers.
- Installation Windows Installer 3.0
- Exécution de Windows Update et installation toutes des mises à jour.
- Installation Microsoft .NET Framework 3.5 Service Pack 1

- **Installation d'ePolicy Orchestrator 4.5**

EPolicy Orchestrator 4.5 est une plate-forme évolutive qui centralise la gestion et la mise en œuvre des stratégies relatives aux produits de sécurité et aux systèmes sur lesquels ils sont installés. Elle propose également des fonctionnalités complètes de déploiement de produits et de génération de rapports, par l'intermédiaire d'un point de contrôle unique.

Pour la procédure d'installation d'EPO Orchestrateur j'ai suivie le guide d'installation proposé par McAfee : ePolicy Orchestrator 4.5 Installation Guide que vous pouvez le trouver sur le lien https://mysupport.mcafee.com/eservice/productdocuments.aspx?strPage=2

.

➢ Installation du service WCF DLP

Le logiciel McAfee Host Data Loss Prevention version 9.0 met en œuvre un service WCF auto-hébergé. Ce nouveau service est plus rapide, plus transparent et plus sécurisé que l'ancien service basé sur le logiciel IIS.

Pour utiliser Windows ou l'authentification SQL avec WCF et la base de données ePO, un utilisateur autorisé doit être défini dans la base de données SQL. L'utilisateur autorisé peut être un utilisateur Windows ou un utilisateur SQL.

Pour effectuer cette tâche, on doit disposer de Microsoft SQL Server Management Studio déjà installés. Âpres cela on passe a installation de DLPWCFServiceInstaller.msi.
Pour test si le service fonctionne bien on utilise la page
http://hôtelocal:8731/DLPWCF/Admin/Testing de navigateur.

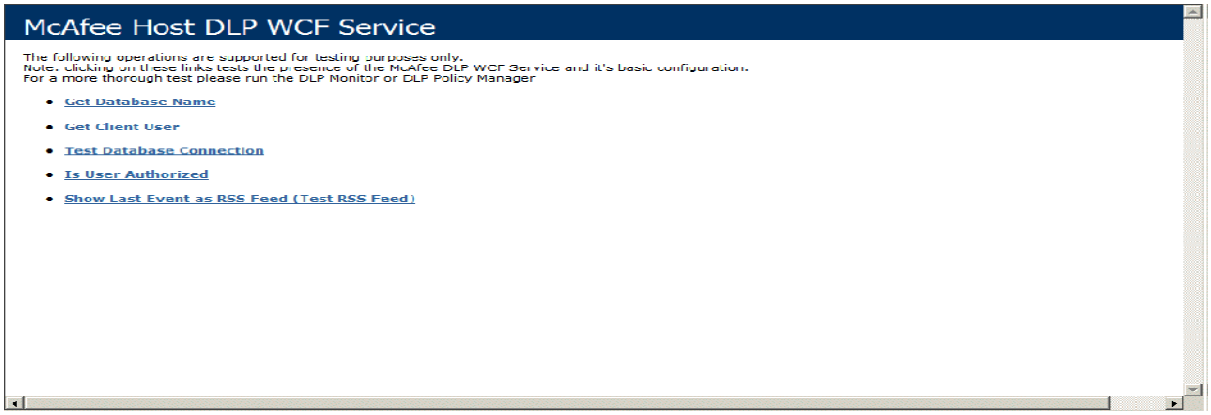


Figure 14 : Page de test du service WCF DLP

2.2 Installation du McAfee Host Data Loss Prevention

Cette partie rassemble les étapes relatives à une nouvelle installation, l'installation par défaut est une licence de 90 jours pour McAfee Device Control. Par l'acquisition d'une licence pour une version complète de McAfee Host Data Loss Prevention, on peut effectue la mise à niveau de la licence après avoir terminé l'installation.

Avant de procéder a l'installation du logiciel McAfee Host Data Loss Prevention, il est nécessaire de saisir certaines informations pour le bon déroulement des opérations. Afin d'éviter toute interruption, parmi ses informations la création de deux dossiers partagés sur réseau, puis configurer les propriétés et les paramètres de sécurité correspondants. Il est généralement préférable (mais non obligatoire) de placer les dossiers sur le même ordinateur que le serveur Host DLP et de base de données. McAfee suggère les chemins d'accès aux dossiers, les noms de dossier et les noms de partage suivants :

• c:\dlp_resources\

• c:\dlp_resources\evidence

• c:\dlp_resources\whitelist

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

- **Dossier Evidence**

Certaines règles de protection permettent de stocker des preuves. On peut crée à l'avance un endroit où les placer. Si, par exemple, un e-mail est bloqué, une copie de ce message est placée dans le dossier Evidence.

- **Dossier Whitelist**

Les empreintes de texte que l'agent DLP doit ignorer sont placées dans un dossier de référentiel de liste d'autorisation. Il s'agit par exemple de petits textes standards adjoints d'office, tels que des décharges de responsabilité ou des avis de copyright. Le logiciel McAfee Host Data Loss Prevention gagne du temps en ignorant ces portions de texte dont il sait qu'elles n'incluent pas de contenu sensible.

Avant de commencer l'installation on doit Vérifier que le nom du serveur ePolicy Orchestrator figure dans la liste des sites de confiance dans les paramètres de sécurité d'Internet Explorer.

Après on suit la procédure suivant :

1- Dans ePolicy Orchestrator, dans **Menu | Logiciels | Extensions**, puis on clique sur **Installer une extension**.
2- **Parcourir** pour rechercher et sélectionner le fichier ZIP du gestionnaire de stratégies (...\HDLP_Extension_9_0_0_xxx.zip). **Ouvrir**, puis sur **OK**. La boîte de dialogue d'installation affiche les paramètres du fichier afin que nous puissions vérifier s'il s'agit bien de l'extension appropriée.
3- On Clique sur **OK**. L'extension est installée. Et Les applications suivantes sont installées :

   • Gestionnaire de stratégies Host DLP

   • Moniteur d'événements Host DLP

   • Analyseur d'événements DLP

4- on suit les mêmes étapes pour installer composant d'aide (...\help_dlp_900.zip).

2.3 Après installation

Plusieurs étapes sont nécessaires pour terminer l'installation du logiciel McAfee Host Data Loss Prevention. la premier étapes la configuration de gestionnaire de stratégies à l'aide d'un assistant tout au long de l'initialisation ensuite installation de McAfee Agent c'est un composant côté client qui permet la communication sécurisée entre les produits McAfee managés et ePolicy Orchestrator.
ePo offre une série de services, tels que la mise à jour, la journalisation, la création de rapports sur les événements et les propriétés, la planification de tâches, la communication et le stockage des stratégies. Exécuté en mode silencieux à l'arrière-plan, l'agent effectue les opérations suivantes :

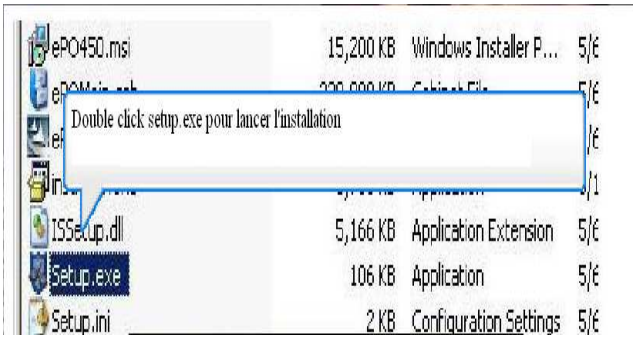
• Il collecte des informations et des événements provenant des systèmes managés et les envoie au serveur ePO.

• Il installe les produits et les mises à niveau sur les systèmes managés.

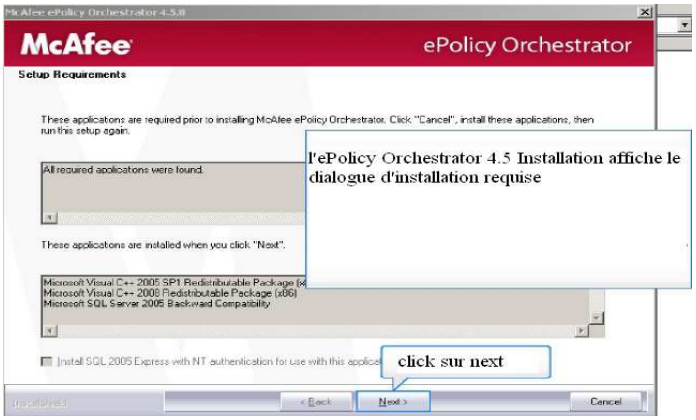
• Il met en œuvre les stratégies et planifie les tâches requises sur les systèmes managés, et il retourne les événements collectés au serveur ePO.

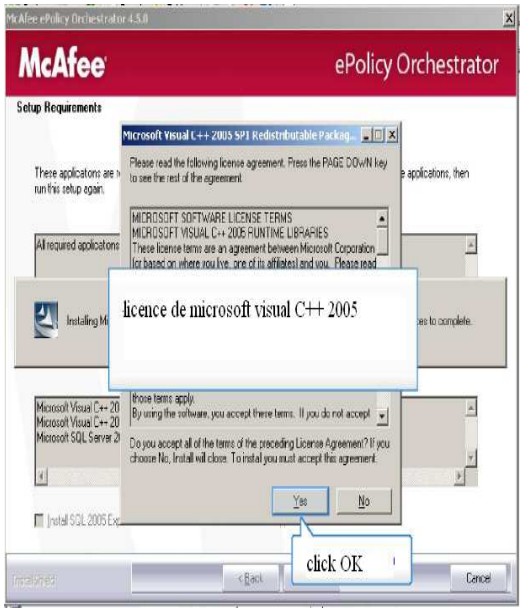
Donc après avoir installé McAfee agent La dernière étape c'est le déploiement de l'agent DLP pour cela McAfee recommande de définir une règle de protection avant le déploiement de l'agent pour tester le système.

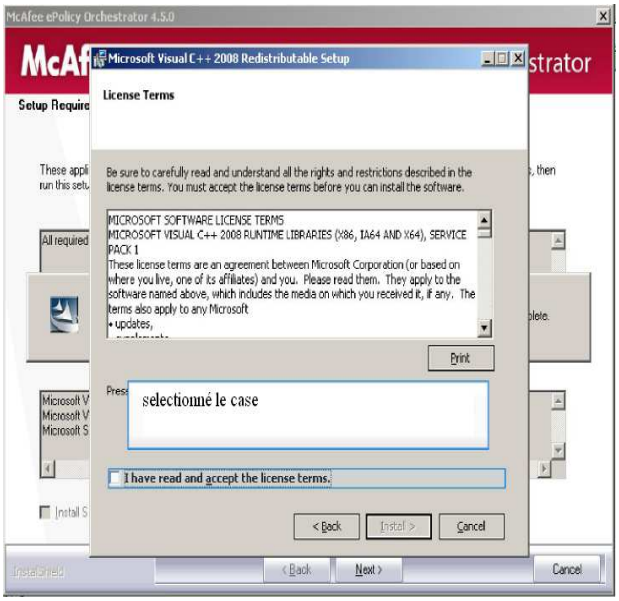
Procédure d'installation de McAfee ePolicy Orchestrator 4.5



cette boite de dialogue indique que Orchestrator4.5 ePolicy ne fournira pas la possibilité d'installer SQL 2005 Express, le programme d'installation a détecté une pré-existante de SQL Server 2005 installé

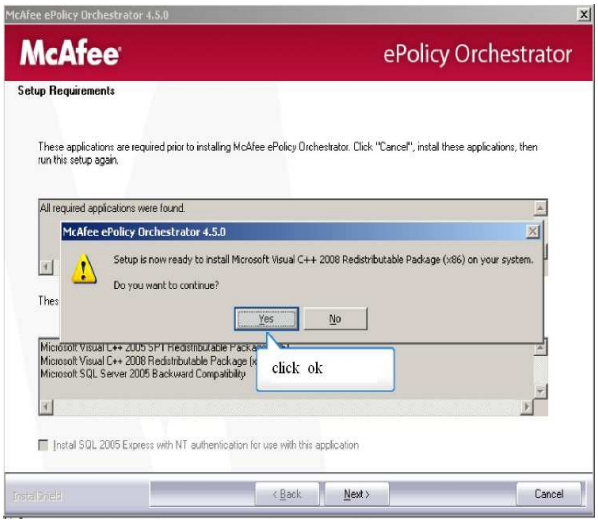



McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Setup Requirements
Microsoft Visual C++ 2005 SP1 Redistributable Packag...
Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT VISUAL C++ 2005 RUNTIME LIBRARIES
licence de microsoft visual C++ 2005
Do you accept all of the terms of the preceding License Agreement? If you choose No, Install will close. To install you must accept this agreement.
Yes
No
click OK
Cancel

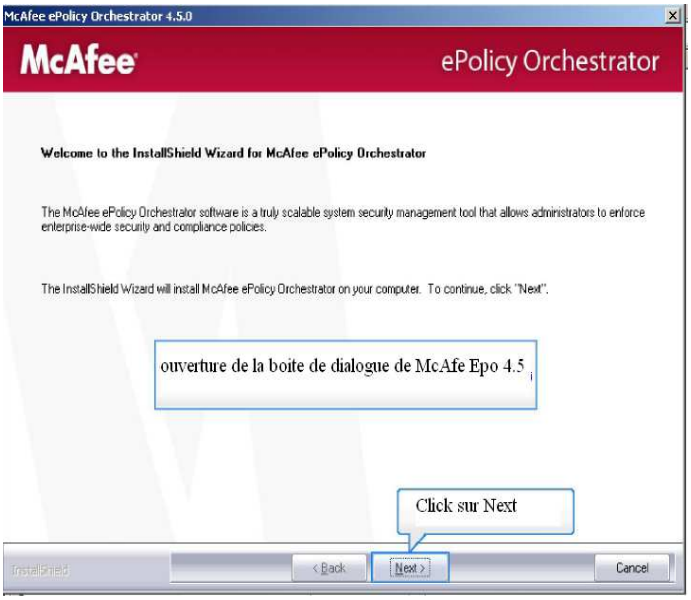

McAfee ePolicy Orchestrator 4.5.0
Microsoft Visual C++ 2008 Redistributable Setup
License Terms
Be sure to carefully read and understand all the rights and restrictions described in the license terms. You must accept the license terms before you can install the software.
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT VISUAL C++ 2008 RUNTIME LIBRARIES (X86, IA64 AND X64), SERVICE PACK 1
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft
Print
selectionné le case
I have read and accept the license terms.
< Back
Install >
Cancel
Next >
Cancel

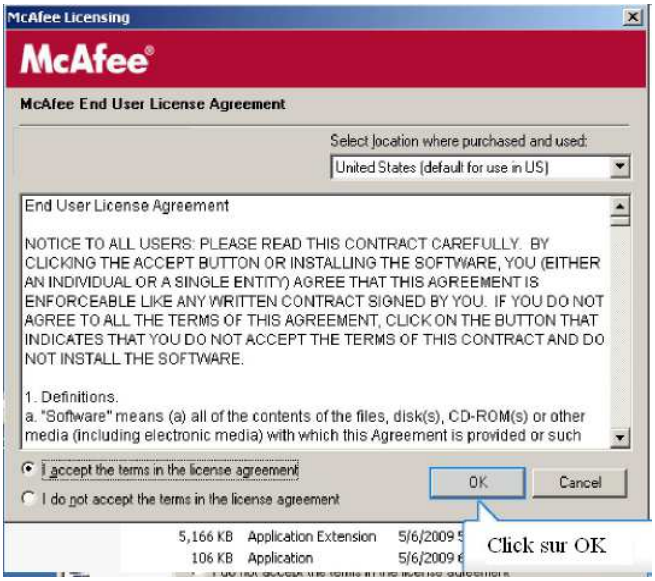
McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Setup Requirements
Microsoft Visual C++ 2005 SP1 Redistributable Packag...
Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.
Installation de microsoft visual C++ 2005
Extracting vcredist.msi
Cancel
Do you accept all of the terms of the preceding License Agreement? If you choose No, Install will close. To install you must accept this agreement.
Yes
No
Next >
Cancel

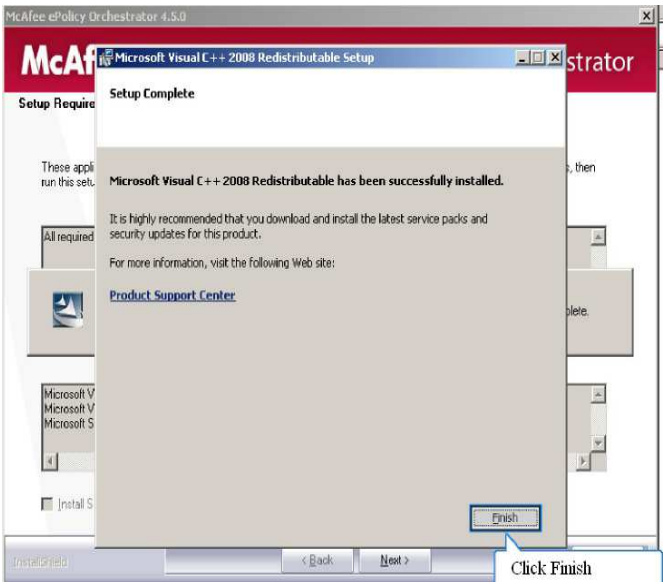
McAfee ePolicy Orchestrator 4.5.0
Microsoft Visual C++ 2008 Redistributable Setup
Welcome to Microsoft Visual C++ 2008 Redistributable Setup
This wizard will guide you through the installation process.
.Setup de Microsoft visual C++ 2008
Next >
Cancel
Click next
Cancel


McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Setup Requirements
These applications are required prior to installing McAfee ePolicy Orchestrator. Click "Cancel", install these applications, then run this setup again.
All required applications were found.
McAfee ePolicy Orchestrator 4.5.0
Setup is now ready to install Microsoft Visual C++ 2008 Redistributable Package (x86) on your system.
Do you want to continue?
Yes
No
click ok
Install SQL 2005 Express with NT authentication for use with this application
< Back
Next >
Cancel

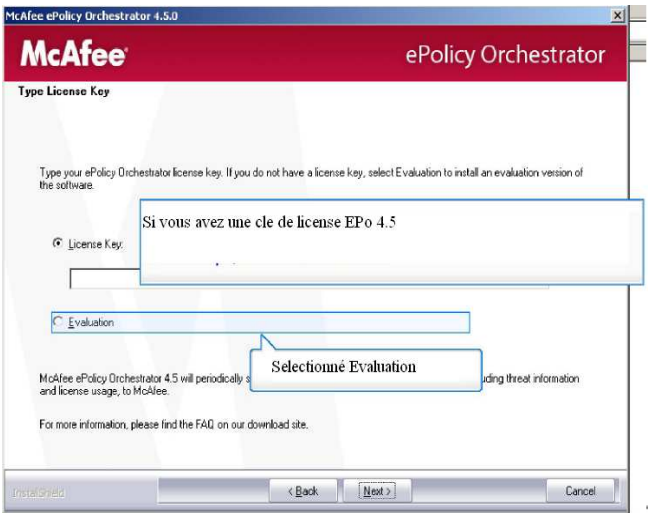
McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
McAfee ePo 4.5 detecte que Microsoft SQL 2005 deja installé et lance installation de SQL server 2005 Bachward compatibility
McAfee ePolicy Orchestrator 4.5.0
Setup is now ready to install Microsoft SQL Server 2005 Backward Compatibility on your system.
Do you want to continue?
Yes
No
click Yes
Install SQL 2005 Express with NT authentication for use with this application
< Back
Next >
Cancel

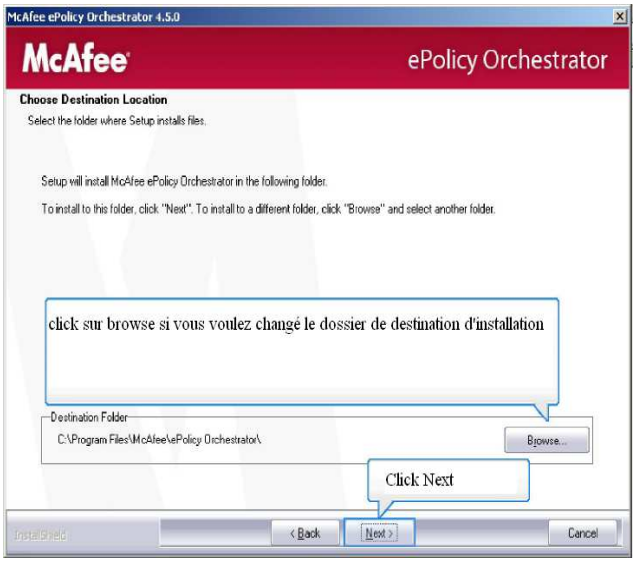

McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Welcome to the InstallShield Wizard for McAfee ePolicy Orchestrator
The McAfee ePolicy Orchestrator software is a truly scalable system security management tool that allows administrators to enforce enterprise-wide security and compliance policies.
The InstallShield Wizard will install McAfee ePolicy Orchestrator on your computer. To continue, click "Next".
ouverture de la boite de dialogue de McAfe Epo 4.5
Click sur Next
< Back
Next >
Cancel

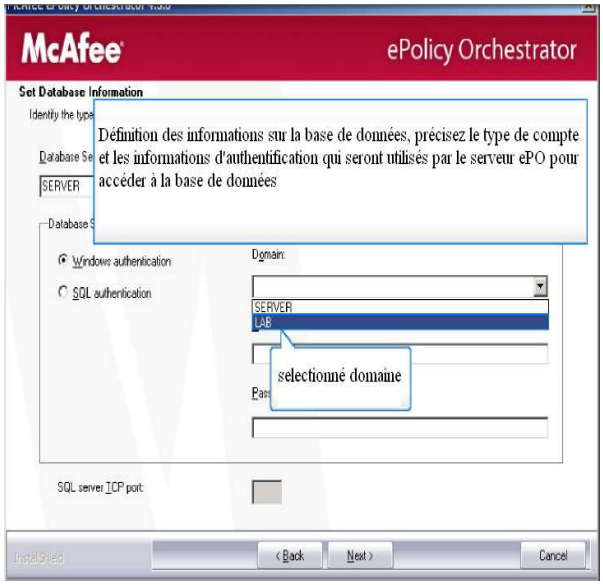

McAfee Licensing
McAfee
McAfee End User License Agreement
Select location where purchased and used:
United States (default for use in US)
End User License Agreement
NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS CONTRACT AND DO NOT INSTALL THE SOFTWARE.
1. Definitions.
a. "Software" means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such
I accept the terms in the license agreement
I do not accept the terms in the license agreement
OK
Cancel
Click sur OK

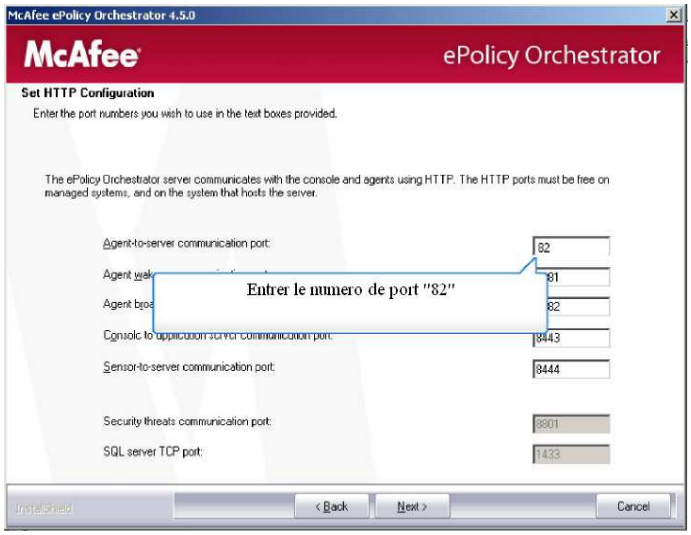

McAfee ePolicy Orchestrator 4.5.0
Microsoft Visual C++ 2008 Redistributable Setup
Setup Complete
Microsoft Visual C++ 2008 Redistributable has been successfully installed.
It is highly recommended that you download and install the latest service packs and security updates for this product.
For more information, visit the following Web site:
Product Support Center
Finish
Click Finish

McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Set Database Information
Identify the type of account and authentication details that the ePO server uses to access the database.
Database Server:
SERVER
Indiqué le nom du server
SQL authentication
User name:
Password:
SQL server TCP port:
< Back
Next >
Cancel

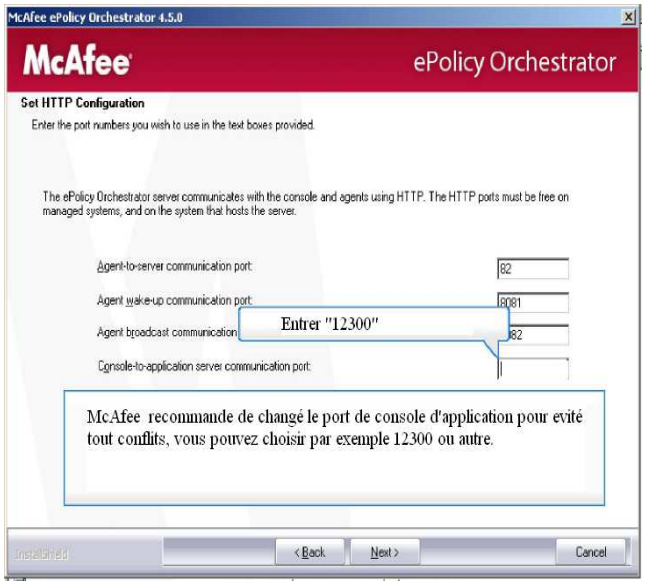

McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Type License Key
Type your ePolicy Orchestrator license key. If you do not have a license key, select Evaluation to install an evaluation version of the software.
Si vous avez une cle de license EPo 4.5
License Key:
Evaluation
Selectionné Evaluation
For more information, please find the FAQ on our download site.
< Back
Next >
Cancel

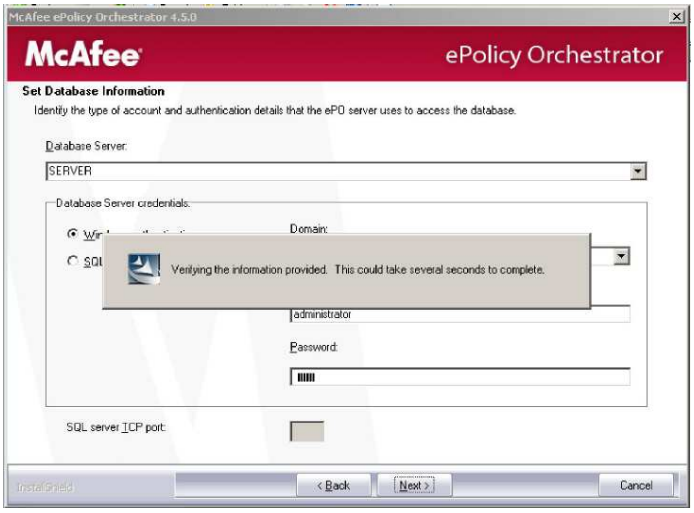

McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Choose Destination Location
Select the folder where Setup installs files.
Setup will install McAfee ePolicy Orchestrator in the following folder.
To install to this folder, click "Next". To install to a different folder, click "Browse" and select another folder.
click sur browse si vous voulez changé le dossier de destination d'installation
Destination Folder
C:\Program Files\McAfee\ePolicy Orchestrator\
Browse...
Click Next
< Back
Next >
Cancel

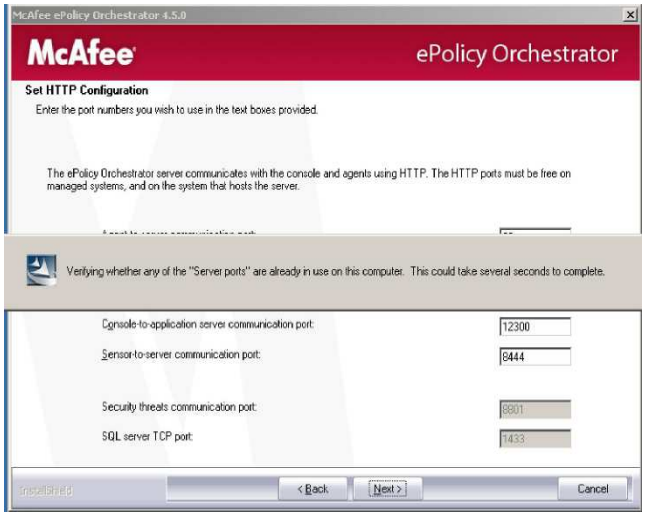

McAfee
ePolicy Orchestrator
Set Database Information
Définition des informations sur la base de données, précisez le type de compte et les informations d'authentification qui seront utilisés par le serveur ePO pour accéder à la base de données
SERVER
Windows authentication
SQL authentication
Domain:
SERVER
LAB
selectionné domaine
SQL server TCP port:
< Back
Next >
Cancel

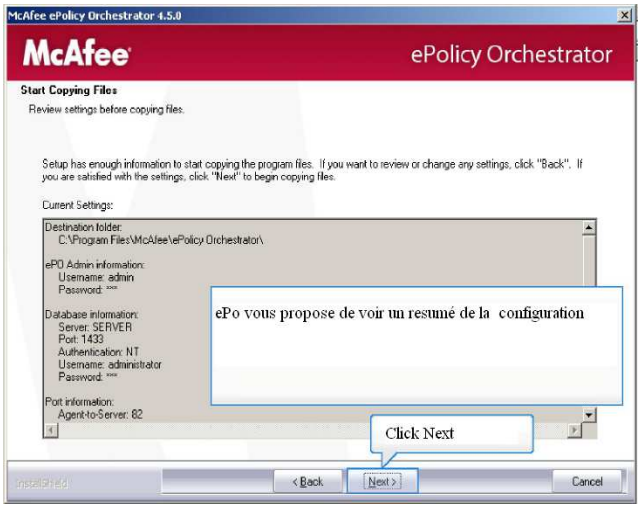

McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Set HTTP Configuration
Enter the port numbers you wish to use in the text boxes provided.
The ePolicy Orchestrator server communicates with the console and agents using HTTP. The HTTP ports must be free on managed systems, and on the system that hosts the server.
Agent-to-server communication port:
82
Entrer le numero de port "82"
8443
Sensor-to-server communication port:
8444
Security threats communication port:
8901
SQL server TCP port:
1433
< Back
Next >
Cancel

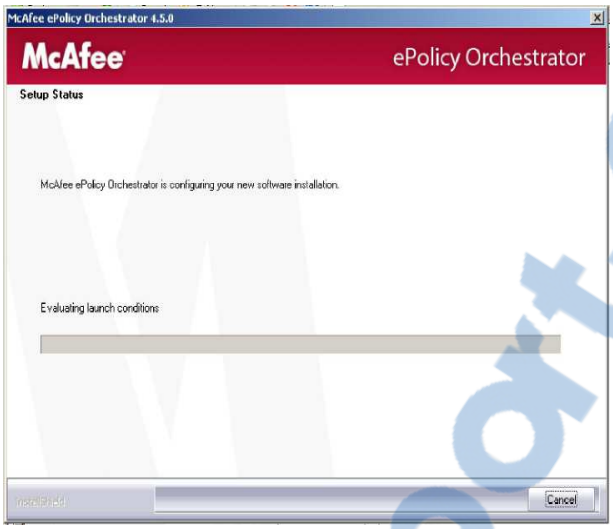
McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Set Database Information
Identify the type of account and authentication details that the ePO server uses to access the database.
Database Server:
Entrer le nom d'un utilisateur administrateur
User name:
administrator
Password:
SQL server TCP port:
< Back
Next >
Cancel

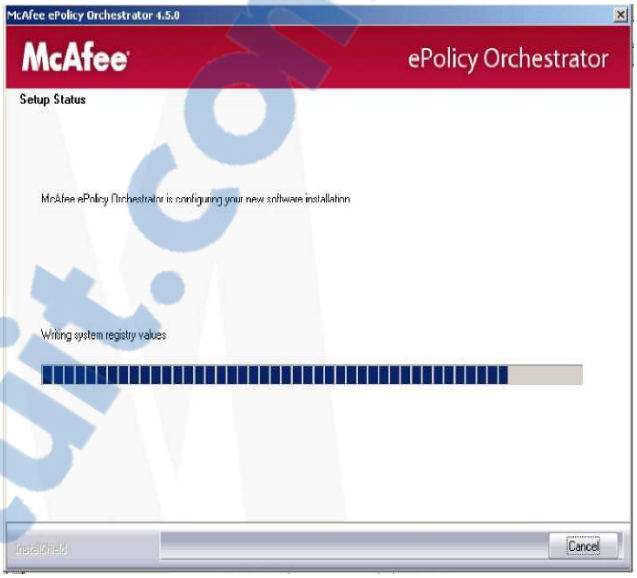

McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Set HTTP Configuration
Enter the port numbers you wish to use in the text boxes provided.
The ePolicy Orchestrator server communicates with the console and agents using HTTP. The HTTP ports must be free on managed systems, and on the system that hosts the server.
Agent-to-server communication port:
82
Agent wake-up communication port:
8081
Entrer "12300"
Console-to-application server communication port:
McAfee recommande de changé le port de console d'application pour evité tout conflits, vous pouvez choisir par exemple 12300 ou autre.
< Back
Next >
Cancel

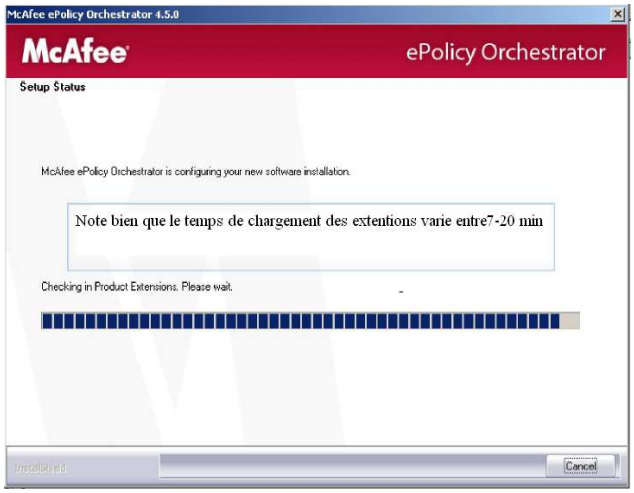

McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Set Database Information
Identify the type of account and authentication details that the ePO server uses to access the database.
Database Server:
SERVER
Database Server credentials:
Domain:
Verifying the information provided. This could take several seconds to complete.
administrator
Password:
SQL server TCP port:
< Back
Next >
Cancel


McAfee ePolicy Orchestrator 4.5.0
McAfee
ePolicy Orchestrator
Set HTTP Configuration
Enter the port numbers you wish to use in the text boxes provided.
The ePolicy Orchestrator server communicates with the console and agents using HTTP. The HTTP ports must be free on managed systems, and on the system that hosts the server.
Verifying whether any of the "Server ports" are already in use on this computer. This could take several seconds to complete.
Console-to-application server communication port:
12300
Sensor-to-server communication port:
8444
Security threats communication port:
8901
SQL server TCP port:
1433
< Back
Next >
Cancel







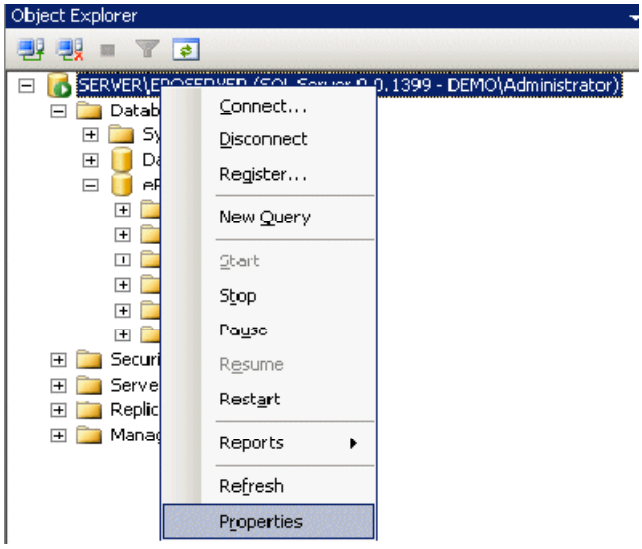


Rapport-Gratuit.com

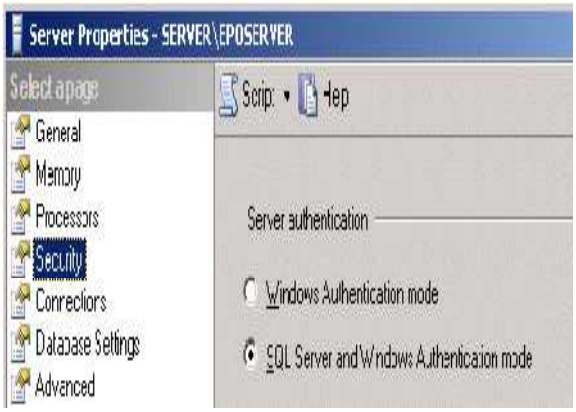
Procédure d'installation de service WCF McAfee

. Ouvrez Microsoft SQL Server Management Studio (Express) et de connecter à l'instance EPOSERVER

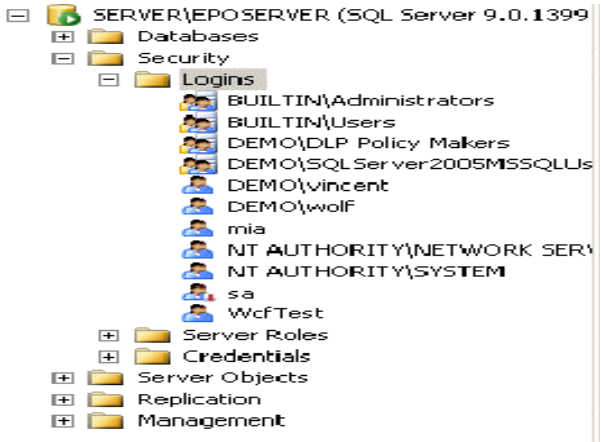
. Click droit sur nom de base de donne et sélectionné propriétés



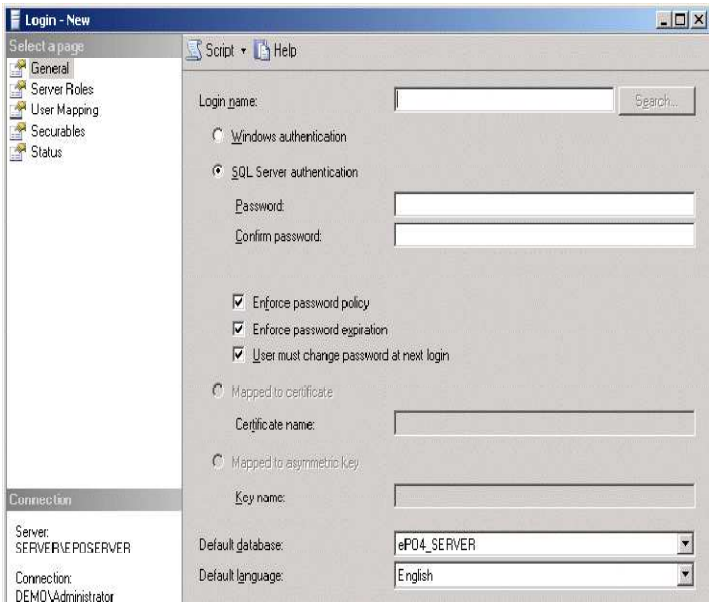
. Sur la page de sécurité, sélectionnez le mode d'authentification Windows ou SQL Server et Mode d'authentification Windows, selon le type d'authentification que vous souhaitez utilisé.



1. Accédez à la sécurité | Connexions. Faites un clic droit dans la page Connexions et sélectionnez Nouvelle connexion

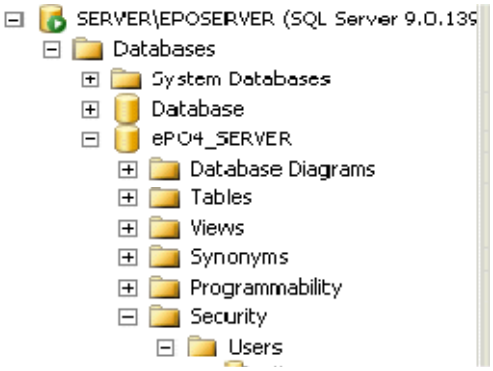


. Sur la page Général de la boîte de dialogue Propriétés de la connexion, sélectionnez l'authentification SQL Server ou l'authentification Windows et tapez un nom de connexion. Définir la base de données par défaut à ePO4_SERVER



. Sur la page de cartographie interactive de la boîte de dialogue Propriétés de la connexion, dans les Utilisateurs mappés à cette section de connexion, sélectionnez ePO4_SERVER et vérifier que l'utilisateur nouveau login est répertorié sous l'utilisateur. Cliquez sur OK.

.Accédez aux bases de données | ePO4_SERVER utilisateur | Sécurité |. Double-cliquez sur la connexion nom d'utilisateur

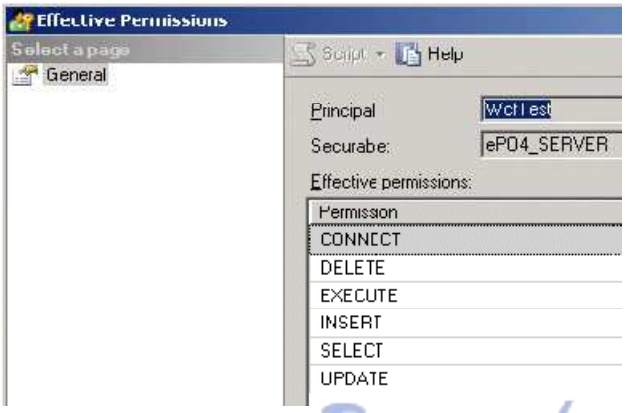


. Sur la page Securables, cliquez sur Ajouter. Sélectionner des objets spécifiques, puis cliquez sur OK.

. Dans la boîte de dialogue Sélectionner les objets, cliquez sur Types d'objets et sélectionné bases de données. Cliquez sur OK.

.Cliquez sur Parcourir. Sélectionnez [ePO4_SERVER] et cliquez sur OK à deux reprises.

. Cliquez Effective autorisations, et vérifier les autorisations suivantes:



Click OK.

. Recherchez et exécutez le programme d'installation DLPWCFServiceInstaller.msi.

. Dans l'Assistant d'installation, procédez comme suit :

Etape	Page	Action
1 sur 6	Présentation	Cliquez sur **Suivant.**
2 sur 6	Licence utilisateur final	Acceptez les conditions, puis cliquez sur **Suivant.**
3 sur 6	Sélection du dossier d'installation	Acceptez l'emplacement par défaut ou **Recherchez** un nouvel emplacement. Cliquez sur **Suivant.**
4 sur 6	Base de données SQL	L'Assistant essaie d'entrer les bonnes données de configuration SQL mais il se peut que vous deviez modifier quelques entrées. Vous devez remplacer l'entrée par défaut de

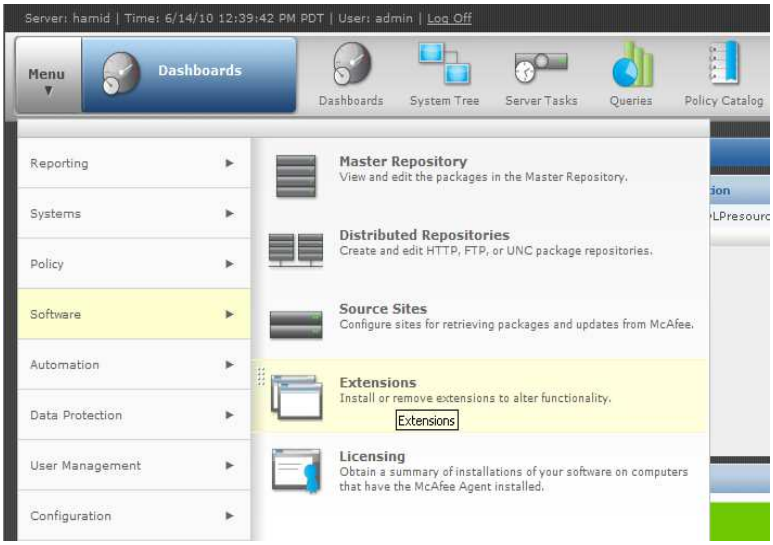
Etape	Page	Action
		Groupes autorisés pour accès web, Tous, par un groupe bénéficiant d'une autorisation d'accès. Cliquez sur **Suivant.**
5 sur 6	Prêt à installer	Revenez en arrière et vérifiez vos paramètres ou cliquez sur **Installer.**
6 sur 6	Fin de la configuration	Cliquez sur **Terminer.**

Pour dépanner le service WCF DLP, utilisez la page :
http://hôtelocal:8731/DLPWCF/Admin/Testing

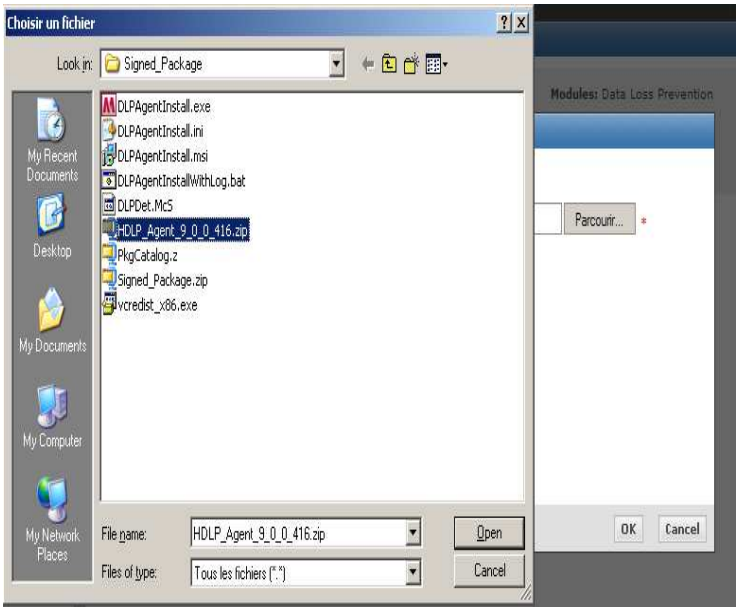
Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

Installation du logiciel McAfee HDLP

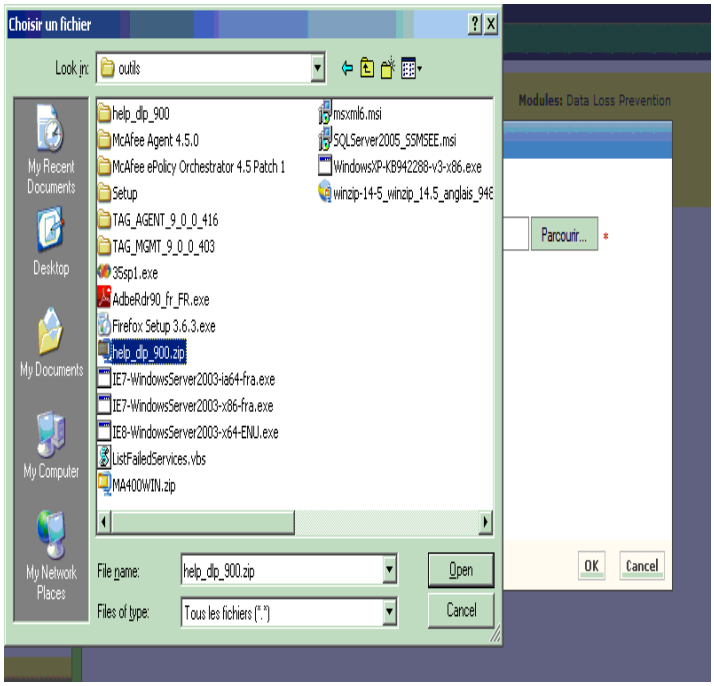
. Dans ePolicy Orchestrator, allez dans Menu | Logiciels | Extensions, puis cliquez sur Installer une extension.



. Cliquez sur Parcourir pour rechercher et sélectionner le fichier ZIP du gestionnaire de Stratégies(...\HDLP_Extension_3_0_0_xxx.zip)

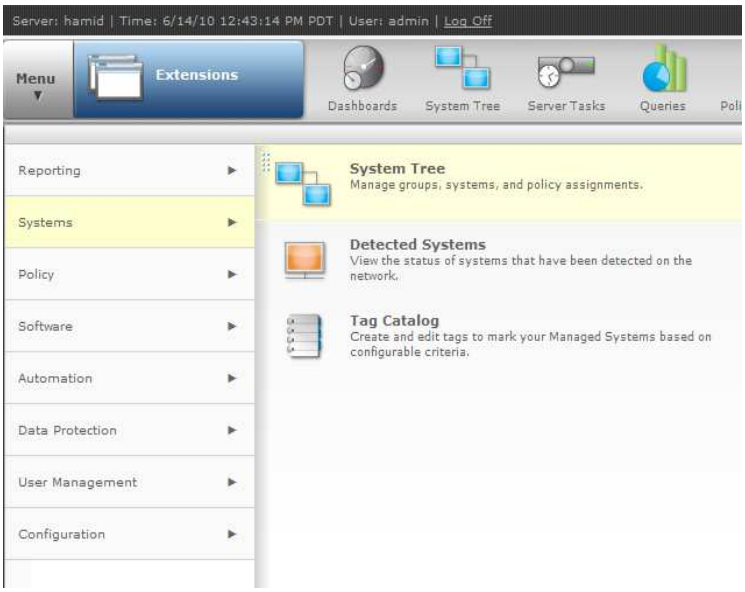


Cliquez de nouveau sur Installer une extension, puis recherchez (option Parcourir) le fichier ZIP d'aide (..\help_dlp_300.zip). Cliquez sur Ouvrir, puis sur OK.
Ce fichier contient l'extension HDLP du système d'aide ePO.

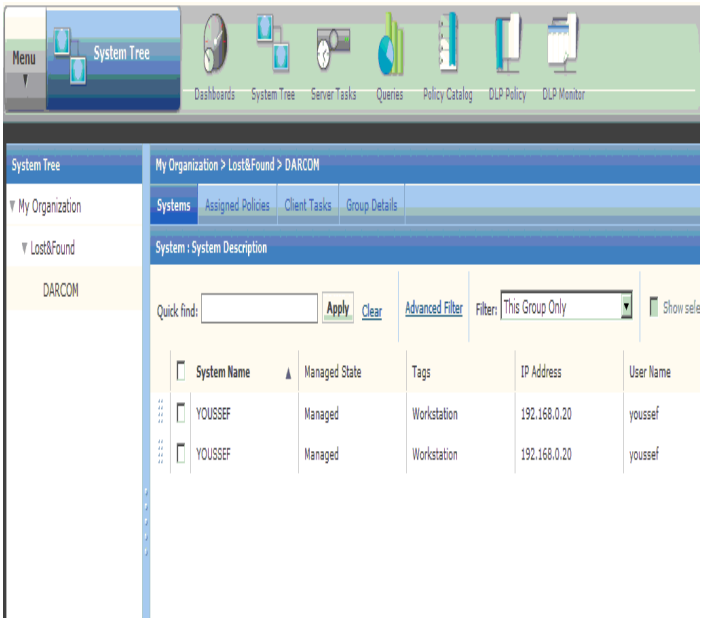


Déploiement de l'agent DLP

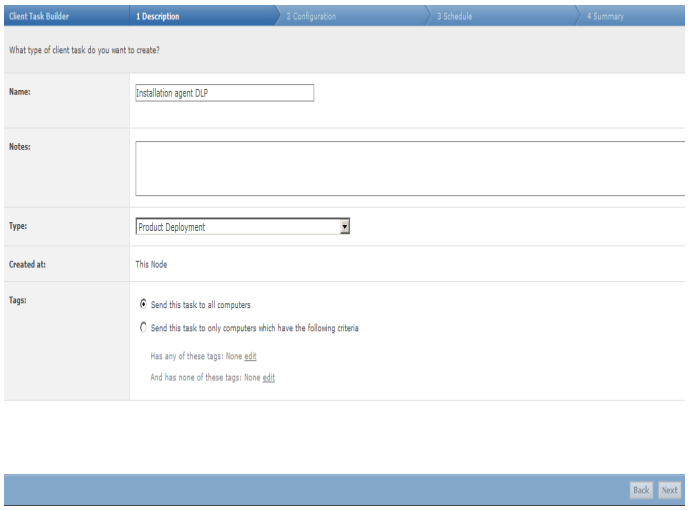
Dans ePolicy Orchestrator 4.5, cliquez sur Arborescence du système.



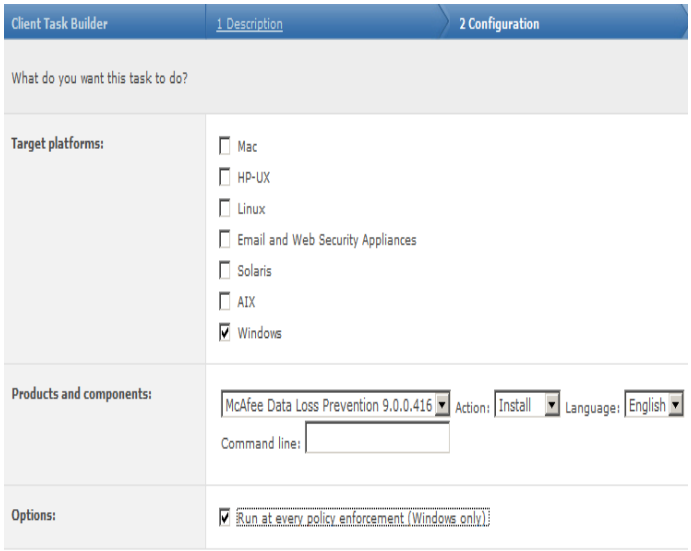
.Dans l'arborescence du système, sélectionnez le niveau de déploiement des agents DLP



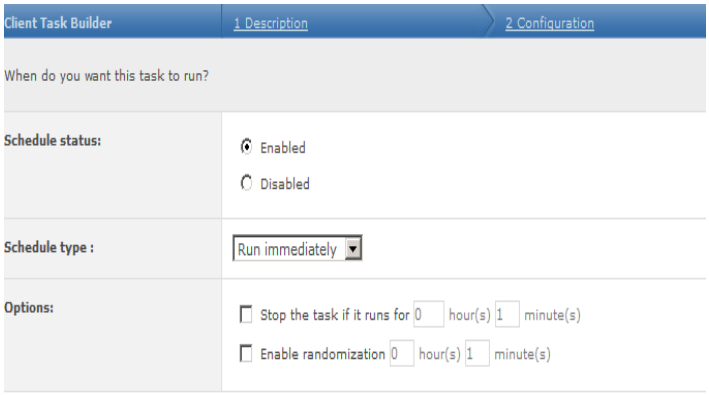
Cliquez sur l'onglet Tâches client. Dans Actions, cliquez sur Nouvelle tâche. Le Générateur de tâches client s'ouvre. Dans la zone Nom, saisissez un nom approprié, par exemple, Installation de l'agent DLP.



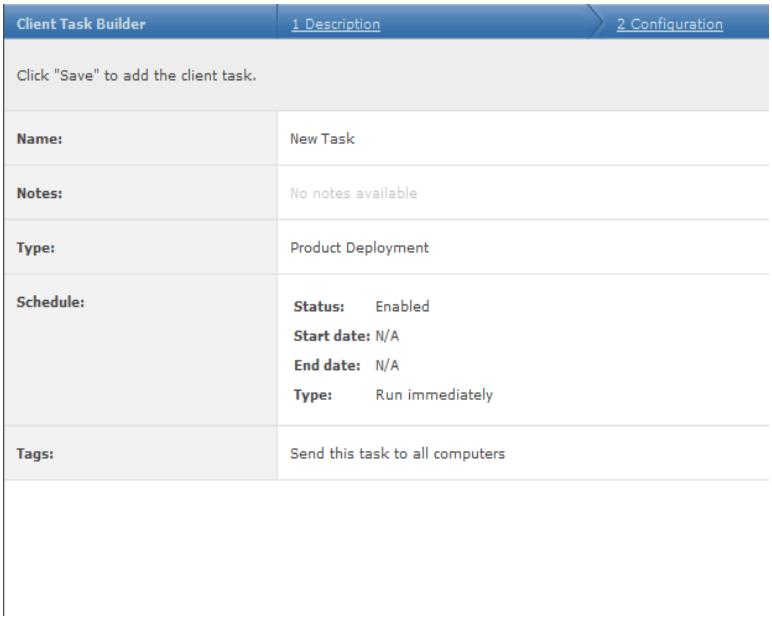
Dans le champ Produits et composants, sélectionnez Data Loss Prevention 9.0.0.0



Définissez le Type de planification sur Exécuter immédiatement. Cliquez sur Suivant



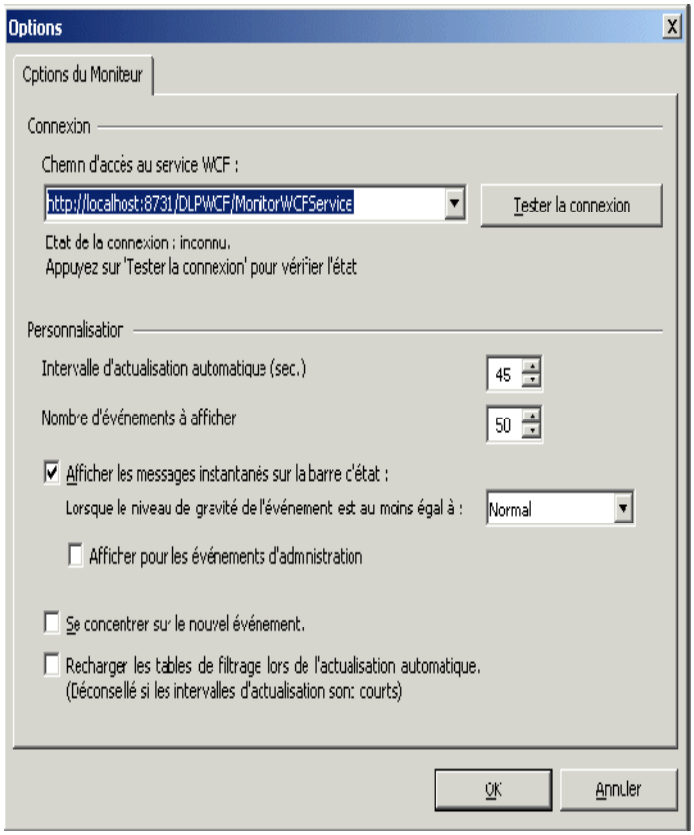
Révisez le récapitulatif de la tâche. Dès que vous êtes satisfait, cliquez sur Enregistrer



Initialisation du moniteur Host DLP

Dans ePolicy Orchestrator 4.5, accédez à Menu | Protection des données | Moniteur DLP.

Pour une installation standard, acceptez les paramètres par défaut. Pour une installation compatible avec les versions antérieures, saisissez l'adresse du service WCF dans la boîte de dialogue. Cliquez sur OK. Le moniteur Host DLP s'ouvre.



3. Classification et suivi de contenu sensible

En matière de sécurité, toutes les données n'ont pas la même importance. La première étape consiste donc à déterminer les plus sensibles - ou celles exposées à des risques supérieurs - afin de prioriser les efforts et politiques de protection. Pour cela il est nécessaire d'avoir une parfaite compréhension de la structure métier de l'entreprise, ses départements et ses lignes d'activités et d'identifier les exigences de sécurité réglementaires et internes applicables à chacun. Une fois le contexte réglementaire et de conformité identifié, il est possible de prioriser les données en les regroupant en « classes » - 1 à 3 par exemple, allant des données les plus sensibles (résultats financiers non publiés) jusqu'aux informations les moins critiques (frais de livraison des fournisseurs, etc.).
McAfee Host Data Loss Prevention vous offre plusieurs méthodes de classification du contenu sensible. Les différentes classifications aident les entreprises à créer le marquage granulaire et les règles de protection permettant de contrôler différents contenus de différentes façons.

La solution McAfee offre trois possibilité pour classifie le contenu à savoir :

3.1 Dictionnaire

Un dictionnaire est un ensemble de mots ou d'expressions clés ; chaque entrée d'un dictionnaire se voit affecter une pondération. Les règles de classification en fonction du contenu utilisent des dictionnaires spécifiés pour classer un document lorsqu'un seuil prédéfini (pondération totale) a été dépassé, c'est à dire, si suffisamment de mots du dictionnaire apparaissent dans le document.

Une règle de marquage de dictionnaire apporte plus de flexibilité ; en effet, on peut définir un seuil, ce qui rend la règle relative. En plus de la possibilité de créer des dictionnaires personnalisés, McAfee Host Data Loss Prevention comprend plusieurs dictionnaires intégrés contenant des termes couramment utilisés dans la santé, les banques, la finance et d'autres secteurs. Les dictionnaires peuvent être créés (et modifiés) manuellement ou par couper/coller à partir d'autres documents.

3.2 Référentiels de documents enregistrés

La fonction de documents enregistrés est une extension du marquage selon l'emplacement.
Elle offre un autre moyen de définir l'emplacement des informations sensibles et d'empêcher qu'elles tombent entre des mains inopportunes de manière non autorisée.
Pour utiliser les référentiels de documents enregistrés, on choisit une liste de dossiers partagés à enregistrer. La définition peut se limiter aux extensions de fichiers spécifiées dans ces dossiers et à une taille de fichier maximale. Le contenu de ces dossiers est classé, marqué d'une empreinte et distribué à tous les postes de travail clients. L'agent Host DLP sur le poste client bloque la diffusion de documents contenant des fragments du contenu enregistré en dehors de l'ordinateur hôte.

3.3 Définitions du modèle textuel

Les règles de marquage et les règles de classification en fonction du contenu utilisent des modèles textuels pour classifier les données en fonction de mots ou de modèles spécifiques. Ils peuvent identifier des chaînes connues (par exemple, « Confidentiel » ou « Usage interne») ou des expressions régulières, qui permettent des comparaisons avec des modèles plus complexes, tels que des numéros de carte de crédit ou de sécurité sociale.

Si plusieurs modèles textuels sont utilisés dans le cadre de comparaisons de contenus similaires, il est possible d'utiliser des groupes de modèles textuels pour associer plusieurs modèles à un même groupe. Cela permet de simplifier la création de catégories de contenu.

3.4 Suivi de contenu

La solution McAfee Host Data Loss Prevention effectue le suivi et contrôle les informations sensibles au moyen de deux mécanismes similaires : les marqueurs et les catégories de contenu. Les règles de marquage permettent d'associer fichiers et données aux marqueurs appropriés. Les règles de classification associent les fichiers et les données aux catégories de contenu. Dans les deux cas, une étiquette est appliquée aux informations sensibles et reste associée au contenu même s'il est copié dans un autre document ou s'il est sauvegardé dans un format différent.

Les marqueurs rendent possible la classification du contenu et l'exploitation pratique de cette classification. Les règles de marquage affectent des marqueurs au contenu issu d'applications ou situé à des emplacements spécifiques. Une fois affectée au contenu, le marqueur reste associé à ce contenu même si ce dernier est déplacé ou copié, s'il est inclus ou joint à d'autres fichiers ou types de fichier. Pour les catégories de contenu s'utilisent avec les règles de classification afin de classifier les groupes de documents enregistrés et le contenu. Elles peuvent également être directement spécifiées dans la plupart des règles de protection.

3.5 Recherche de fichiers présentant du contenu sensible

Cette section décrit les différentes méthodes permettant de rechercher et de définir les fichiers qui contiennent des données sensibles. « Données au repos » est le terme utilisé pour décrire les emplacements effectifs (« où se trouve-t-il dans le réseau ? », « dans quel dossier se trouve-t-il ? »). On peut également définir le contenu en fonction de l'extension de fichier ou de l'application qui a servi à sa création. Cette opération est appelée « données en cours d'utilisation ». Ces définitions nous apportent la granularité qui nous permettra de protéger uniquement les fichiers qui le nécessitent.
Tout cela grâce à DLP Discovery un robot qui s'exécute sur les machines clientes. Lorsqu'il détecte du contenu prédéfini, il peut surveiller, mettre en quarantaine, chiffrer ou supprimer les fichiers concernés.

NB: pour utiliser DLP Discovery, vous devez activer le module de détection dans l'onglet Divers de la boîte de dialogue Configuration des agents.

Il existe deux façons de définir du contenu sensible.

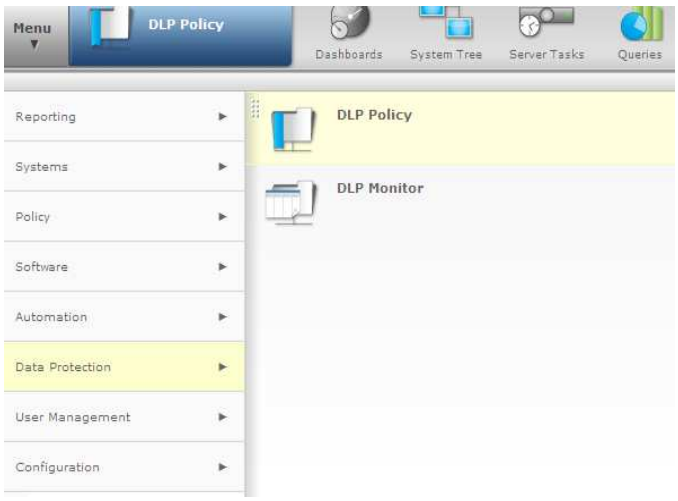
• **Utilisation des catégories de contenu :** Les catégories permettent de faire correspondre aux fichiers des modèles textuels spécifiques, des dictionnaires ou des référentiels de documents enregistrés.

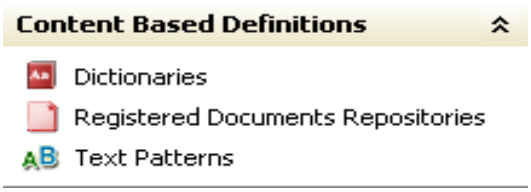
• **Utilisation du contexte de fichier :** les types et les extensions de fichier, les propriétés des documents, le type de chiffrement et l'affectation des utilisateurs dans la règle de découverte.

DLP Discovery du logiciel McAfee Host Data Loss Prevention recherche dans les lecteurs locaux de l'ordinateur client uniquement. Ainsi nous pouvons spécifier les dossiers à analyser avec la taille maximale et ceux à ignorer avec un outil de planification qui nous permet de lancer une analyse à une heure précise chaque jour ou uniquement les jours de la semaine ou du mois que nous aurons spécifiés. On peut préciser les dates de départ et d'arrêt ou exécuter une analyse lorsque la configuration des agents DLP est appliquée, suspendre une analyse lorsque le processeur ou la mémoire RAM de l'ordinateur dépasse une limite définie. Dans le cas ou l'ordinateur est redémarre lorsqu'une analyse est en cours, l'analyse reprend à l'endroit où elle a été interrompue.

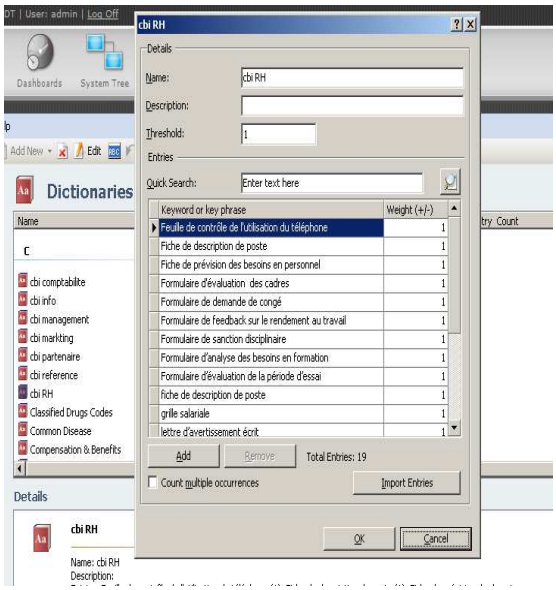
Définition du contenu sensible

Accéder a l'ongle stratégies DLP : Menu |Protection de données | stratégies DLP

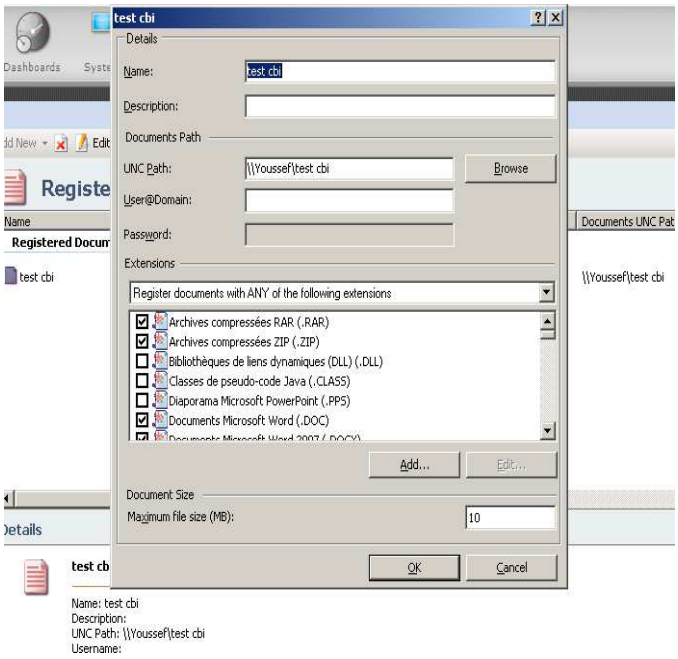




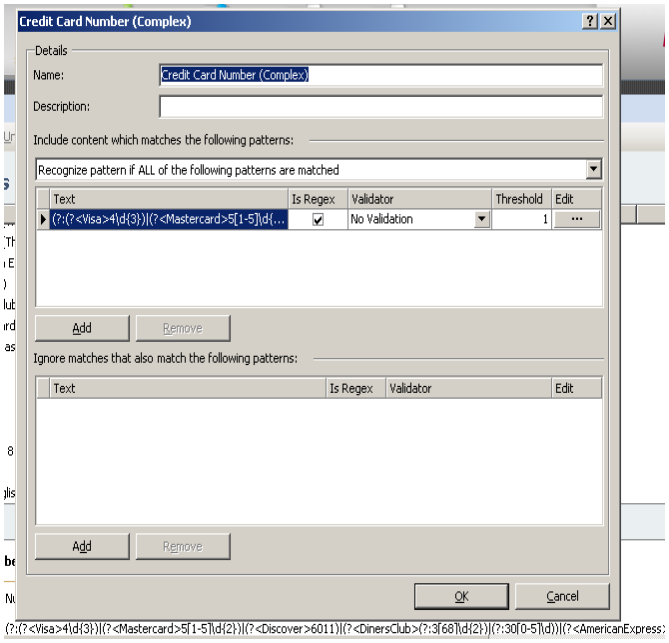
- **Création d'un Dictionnaire**



- **Référentiels de documents enregistrés**



- **modèle textuel**



4. Règles de protection

Les règles de protection contrôlent le flux des données en définissant l'action effectuée en cas de tentative de transfert ou de transmission de données sensibles. Cette opération s'effectue en liant les actions aux définitions, aux marqueurs et aux catégories de contenus ainsi qu'aux groupes d'affectation d'utilisateurs.

La règle de protection spécifie la méthode de transfert, les marqueurs nommés et la réaction du système face à l'événement. Dans certains cas, les règles de protection enregistrent simplement l'événement dans un journal. Dans d'autres, elles peuvent bloquer le transfert des données et avertir l'utilisateur de l'infraction à la stratégie.par la suite je vais vous présente les différentes règles de protection inclus dans la maquette de test réalisée.

Parmi les règles de protection offrir par cette solution La règle de protection de l'accès aux fichiers par les applications qui permettent de surveiller ou bloquer des fichiers en fonction de l'application ou des applications qui les a créés. Comme un exemple clair, utilisation de logiciels pour la conception électroniques (désigne, layout). La deuxième c'est la règle de protection du Presse-papiers (copier /coller) qui surveille ou bloque l'utilisation du Presse-papiers même pour les Presse-papiers de plus d'un mégaoctet qu'on peut l'activé dans l'onglet Configuration avancée de la boîte de dialogue Configuration des agents. Juste une remarque, elle ne fonctionne pas si je colle dans le même type de document, à savoir si je copie à partir de Word, il est bloqué à tout sauf à partir de Word. Ou Excel.

Le troisième risque fréquent réside dont l'utilisation des emails, pour cela des règles de protection des e-mails surveillent ou bloquent les messages envoyés à des adresses ou à des utilisateurs spécifiques.

Ensuite les règles de protection du système de fichiers protègent les fichiers présents sur des serveurs de fichiers ou des périphériques de stockage de masse spécifiques. Les fichiers peuvent être surveillés mais pas bloqués. Ce qui permet d'enregistrer des preuves et avertir l'utilisateur.

Certain utilisateurs se servir des outils de création de PDF/d'image comme pdf-creator, La solution McAfee Host Data Loss Prevention version 9.0 bloquent les pilotes d'impression de l'outil de création de PDF et d'image qui impriment sur les fichiers. Restant dans le même domaine d'application avec la règle de protection de l'impression qui surveille ou bloque l'impression des fichiers soit pour des imprimantes locaux ou partage dans le réseau.

Les périphériques connectés aux ordinateurs gérés de l'entreprise (téléphones intelligents, périphériques de stockage amovibles, périphériques Bluetooth, baladeurs MP3 ou autres périphériques Plug-and-Play) peuvent être surveillés ou bloqués en utilisant les règles de périphérique qui permettent de surveiller et de contrôler leur utilisation dans la distribution des informations sensibles. Pour la plupart des organisations, ce niveau de prévention des fuites de données est le principal objectif. Il s'agit du niveau de protection apporté par McAfee Device Control.

Une règle de périphériques comprend une liste des définitions de périphériques inclus ou exclus de la règle ainsi que l'action entreprise lorsque la règle est déclenchée par du contenu envoyé vers ou en provenance du périphérique désigné.
En outre, on peut créer différents ensembles de règles pour le personnel de l'entreprise, en fonction des rôles et des besoins. On pourrait imaginer, par exemple, que la majeure partie des employés ne puisse pas copier des données de l'entreprise sur un périphérique de stockage amovible, tandis que le personnel informatique et les commerciaux, en revanche, peuvent utiliser ces périphériques et font uniquement l'objet d'une surveillance par le système. Ce type de scénario peut être mis en œuvre grâce aux propriétés spécifiques du périphérique associées à une règle de périphérique appropriée.

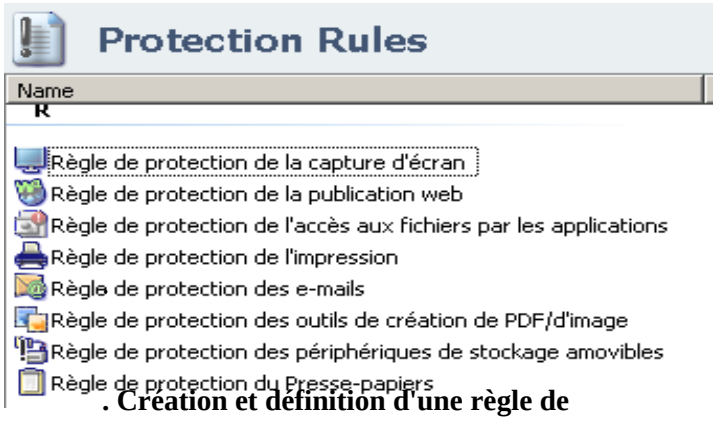
Les règles de protection pour la publication web surveillent ou bloquent la publication des données sur des sites web, y compris les sites de messagerie (Hotmail, gmail).ils prisent en charge pour Microsoft Internet explorer IE6 ou versions ultérieures et Firefox, la dernière règle de protection celle de capture d'écran.

Rapport-Gratuit.com

	Bloquer	Chiffrer	Supprimer	Moniteur	Avertir l'utilisateur	Quarantaine	Lecture seule	Justification de la requête	Enregistrer les preuves
Règle des périphériques Plug-and-Play	●			●	●				
Règle des périphériques de stockage amovibles	●			●	●		●		
Règles de protection de l'accès aux fichiers par les applications				●	●				
Règles de protection du Presse-papiers	●								
Règles de protection de la messagerie	●			●	●			●	●
Règles de protection du système de fichiers	●	●			●				●
Règles de protection de la communication réseau	●			●	●				
Règles de protection des outils de création de PDF/d'image	●			●	●				
Règles de protection de l'impression	●			●	●				●
Règles de protection des périphériques de stockage amovibles	●	●		●	●				●
Règles de protection de la capture d'écran	●			●	●				●
Règles de protection pour la publication web	●			●	●			●	●
Règles de découverte		●	●	●		●			●

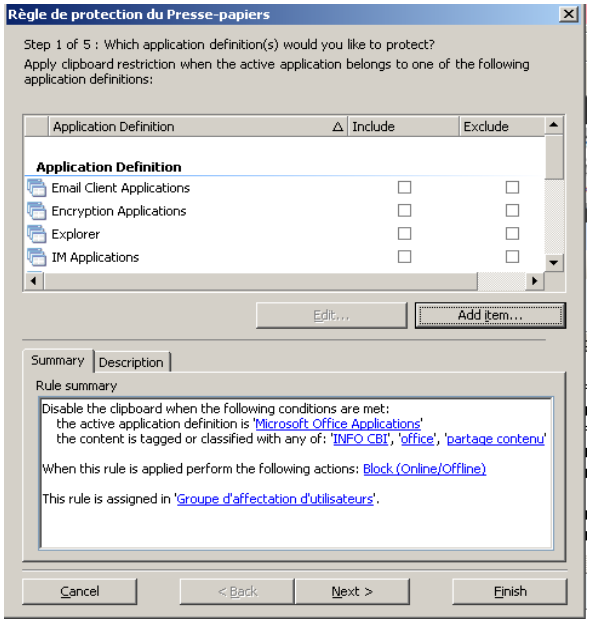
Figure 15 : Règles et actions associées

Définition des règles de protection

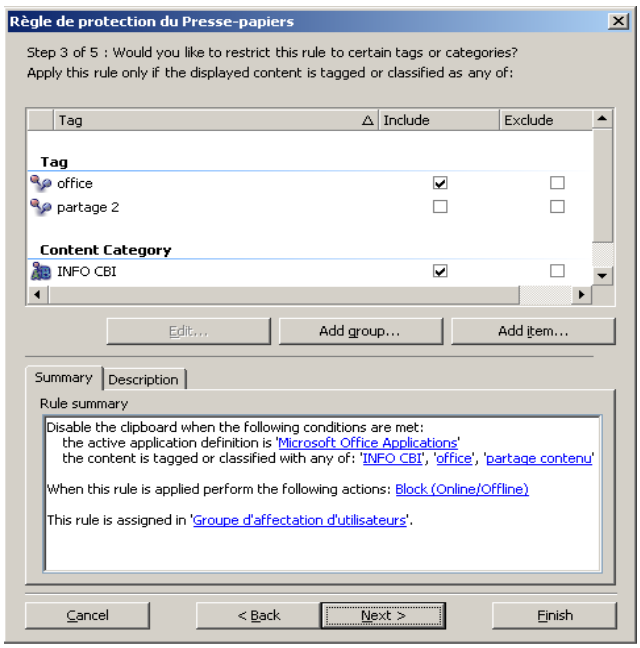


. Création et définition d'une règle de protection du Presse-papiers

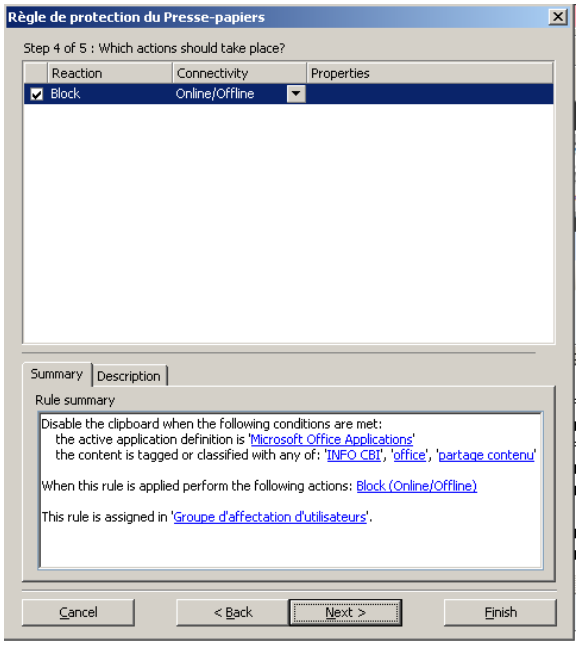
Dans la barre de navigation, sélectionnez Règles | Règles de protection. Les règles de protection disponibles s'affichent dans le volet principal. Sélectionnez une ou plusieurs définitions d'applications dans la liste. Vous pouvez inclure ou exclure définitions. Cliquez sur Ajouter un élément pour créer une définition d'application. Cliquez sur Suivant.



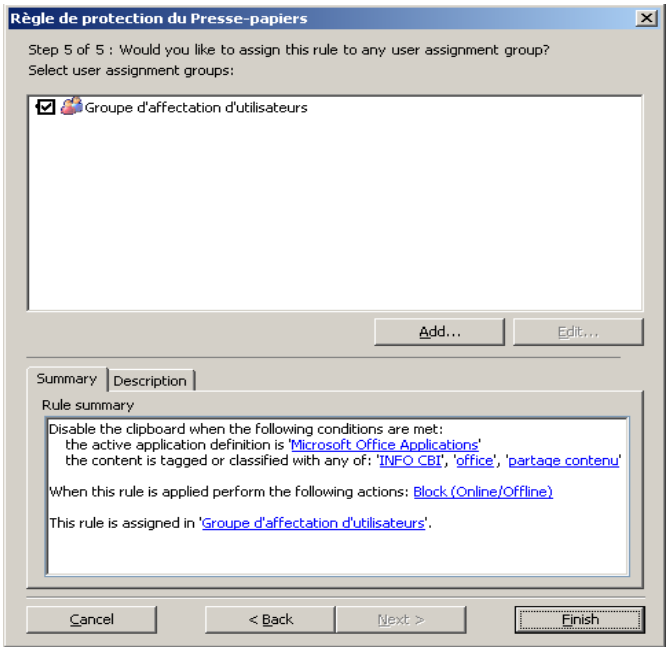
Choisissez Sélectionner dans la liste, puis sélectionnez un Marqueur, une Catégorie de contenu ou un Groupe de marqueurs et de catégories pour cette règle. Cliquez sur Suivant.



Sélectionnez une action dans la liste. Pour les règles de protection du Presse-papiers, la seule action est Bloquer et la seule option est En ligne / Hors ligne. Cliquez sur Suivant.

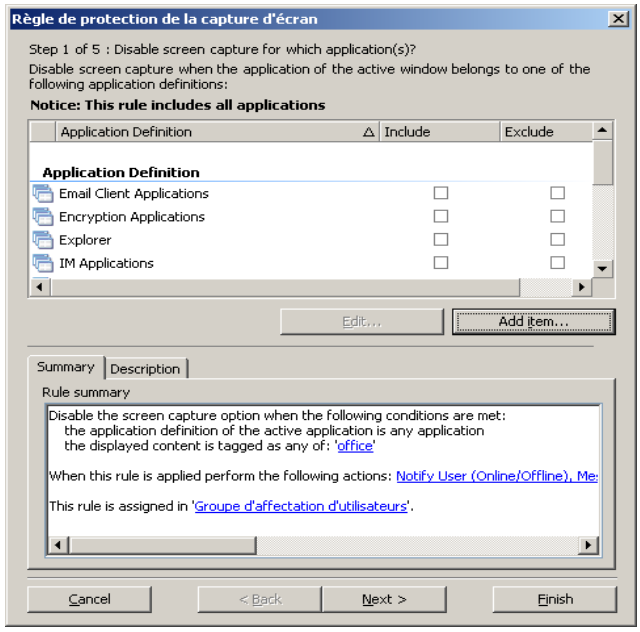


Sélectionnez un ou plusieurs groupes d'affectation puis sur terminer

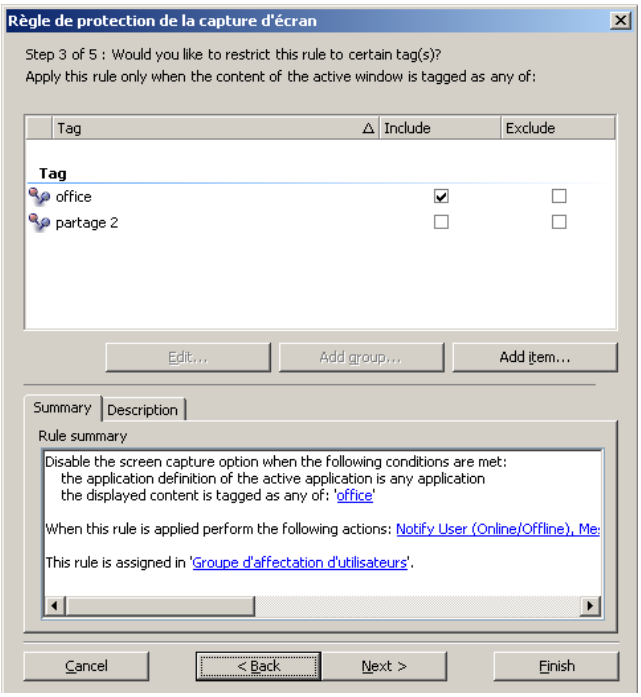


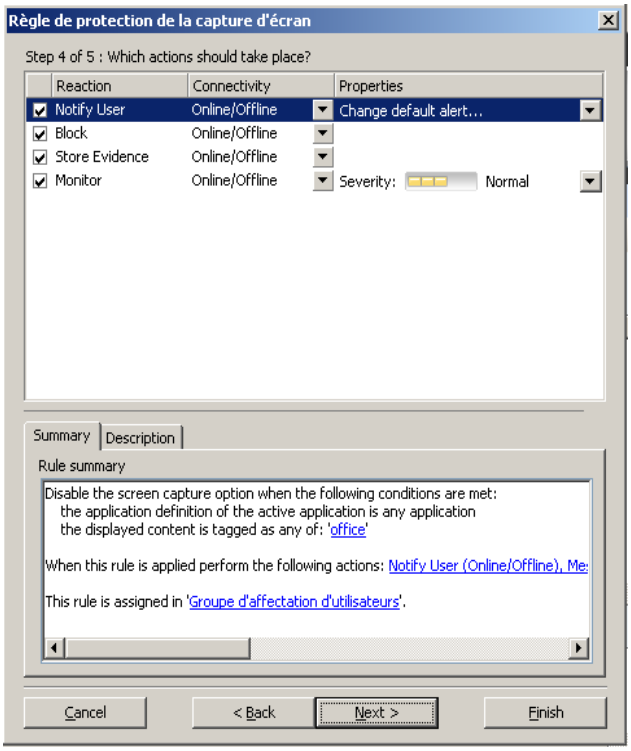
Règle de protection de la capture d'écran.

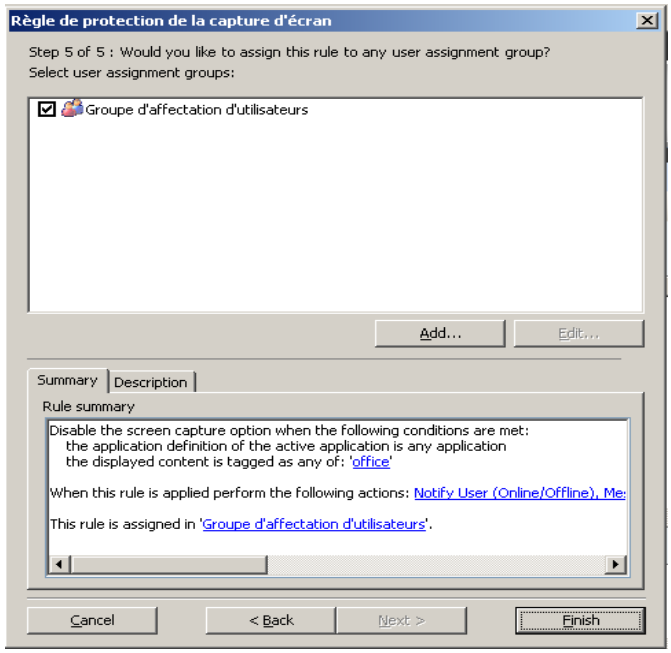
Dans le volet Règles de protection, cliquez avec le bouton droit de la souris, puis sélectionnez Nouveau | Règle de protection de la capture d'écran.



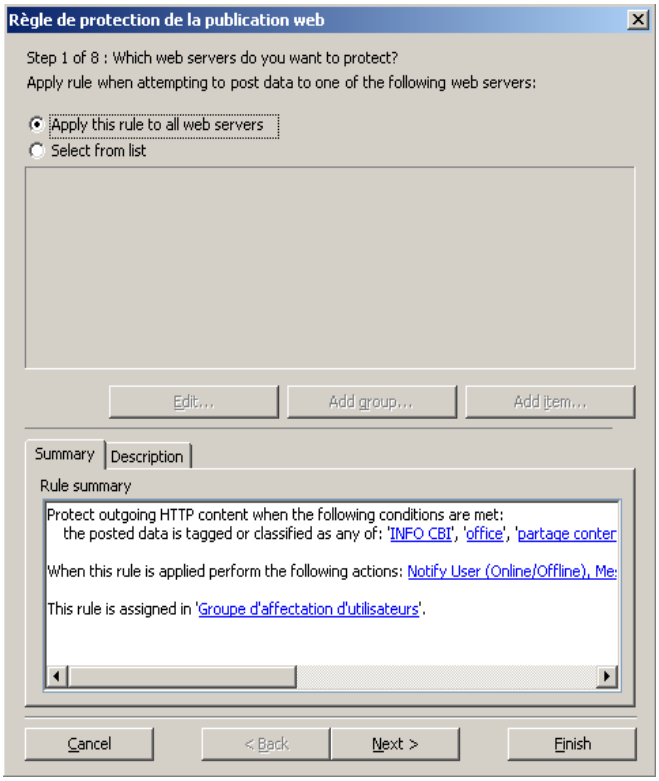
Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

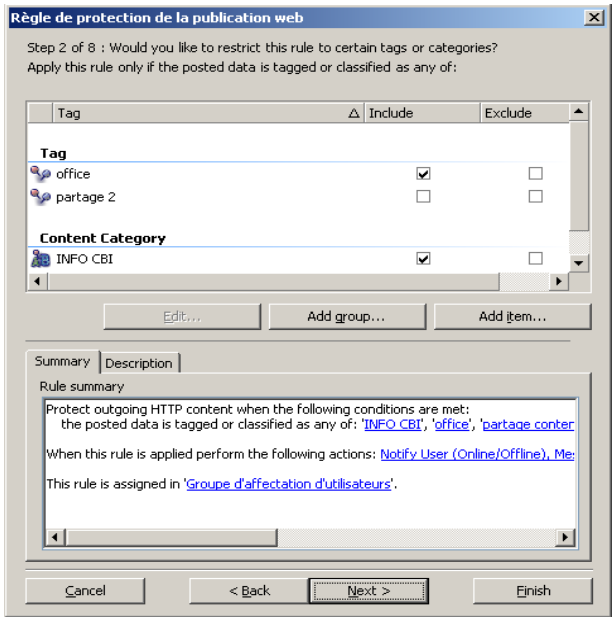


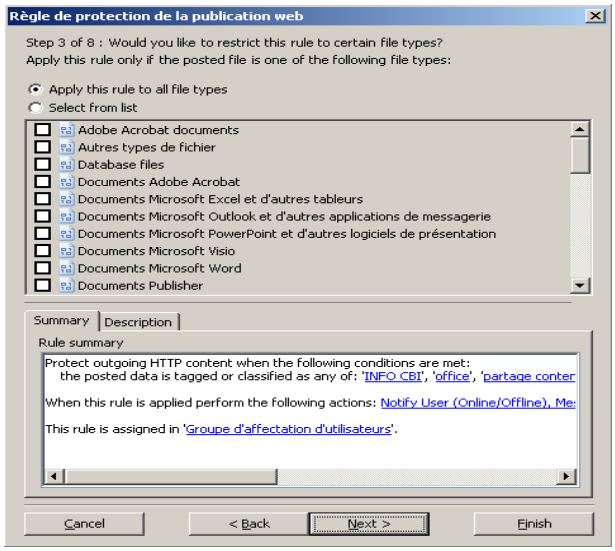


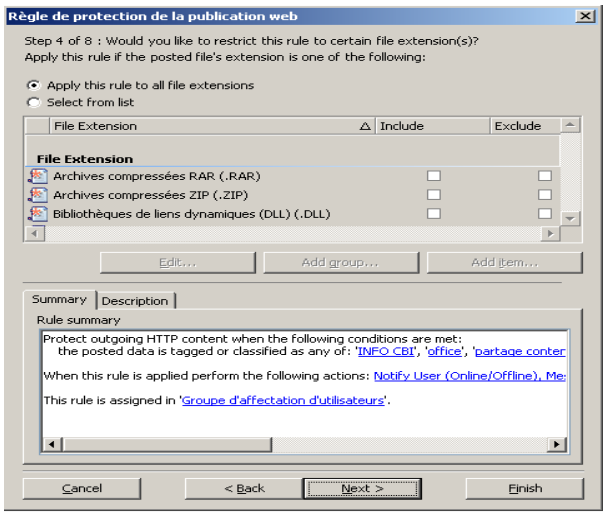


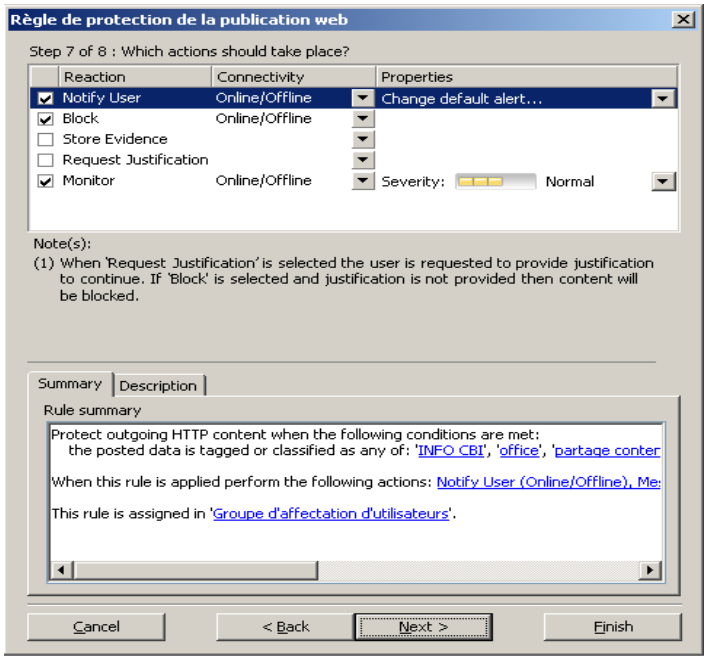
. Règle de protection de la publication Web

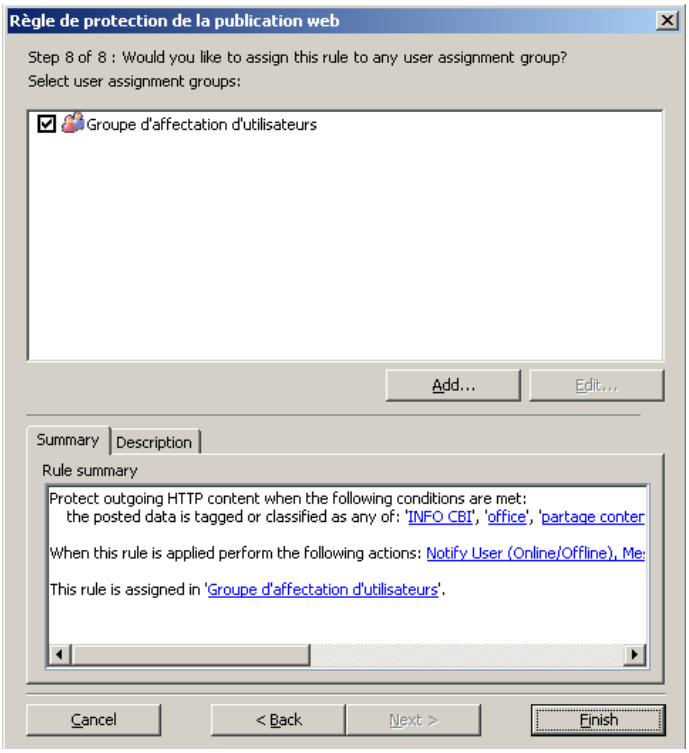



Règle de protection de la publication web
Step 2 of 8 : Would you like to restrict this rule to certain tags or categories?
Apply this rule only if the posted data is tagged or classified as any of:
Tag
Include
Exclude
Tag
office
partage 2
Content Category
INFO CBI
Edit...
Add group...
Add item...
Summary
Description
Rule summary
Protect outgoing HTTP content when the following conditions are met:
the posted data is tagged or classified as any of: 'INFO CBI', 'office', 'partage conter
When this rule is applied perform the following actions: Notify User (Online/Offline), Me
This rule is assigned in 'Groupe d'affectation d'utilisateurs'.
Cancel
< Back
Next >
Finish

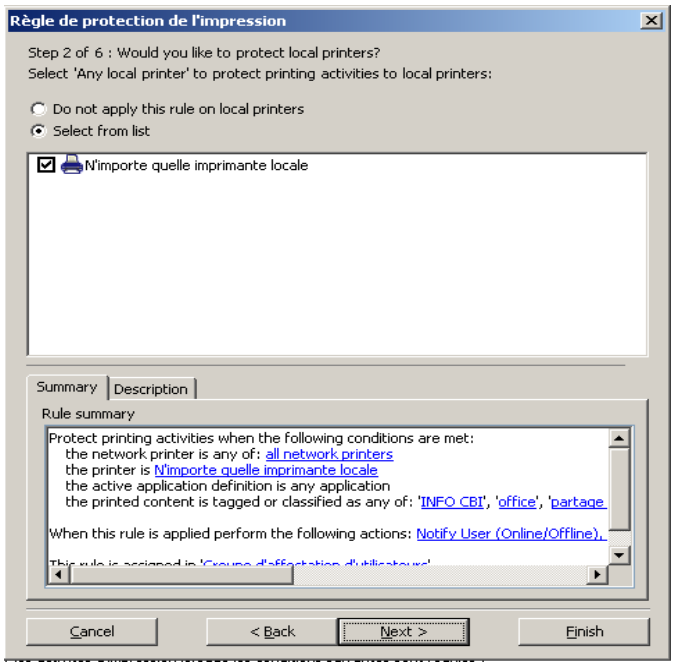

Règle de protection de la publication web
Step 3 of 8 : Would you like to restrict this rule to certain file types?
Apply this rule only if the posted file is one of the following file types:
Apply this rule to all file types
Select from list
Adobe Acrobat documents
Autres types de fichier
Database files
Documents Adobe Acrobat
Documents Microsoft Excel et d'autres tableurs
Documents Microsoft Outlook et d'autres applications de messagerie
Documents Microsoft PowerPoint et d'autres logiciels de présentation
Documents Microsoft Visio
Documents Microsoft Word
Documents Publisher
Summary
Description
Rule summary
Protect outgoing HTTP content when the following conditions are met:
the posted data is tagged or classified as any of: 'INFO CBI', 'office', 'partage conter
When this rule is applied perform the following actions: Notify User (Online/Offline), Me
This rule is assigned in 'Groupe d'affectation d'utilisateurs'.
Cancel
< Back
Next >
Finish

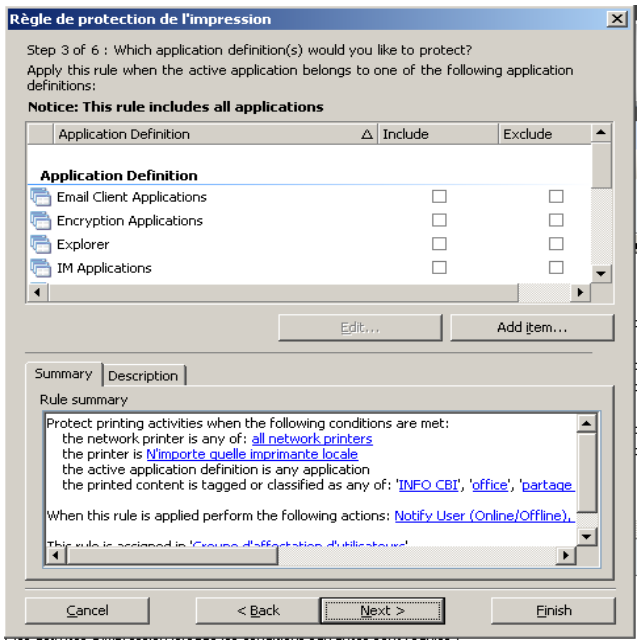

Règle de protection de la publication web
Step 4 of 8 : Would you like to restrict this rule to certain file extension(s)?
Apply this rule if the posted file's extension is one of the following:
Apply this rule to all file extensions
Select from list
File Extension
Include
Exclude
File Extension
Archives compressées RAR (.RAR)
Archives compressées ZIP (.ZIP)
Bibliothèques de liens dynamiques (DLL) (.DLL)
Edit...
Add group...
Add item...
Summary
Description
Rule summary
Protect outgoing HTTP content when the following conditions are met:
the posted data is tagged or classified as any of: 'INFO CBI', 'office', 'partage conter
When this rule is applied perform the following actions: Notify User (Online/Offline), Me
This rule is assigned in 'Groupe d'affectation d'utilisateurs'.
Cancel
< Back
Next >
Finish

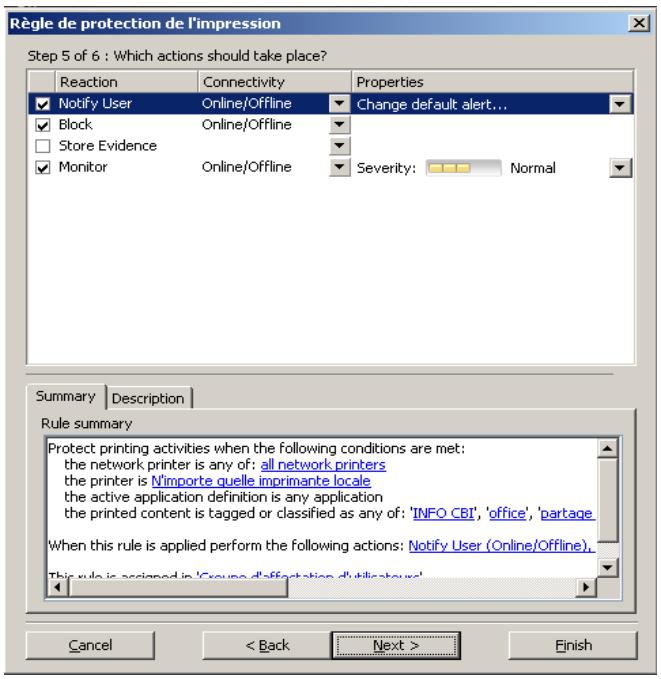

Règle de protection de la publication web
Step 7 of 8 : Which actions should take place?
Reaction
Connectivity
Properties
Notify User
Online/Offline
Change default alert...
Block
Online/Offline
Store Evidence
Request Justification
Monitor
Online/Offline
Severity:
Normal
Note(s):
(1) When 'Request Justification' is selected the user is requested to provide justification to continue. If 'Block' is selected and justification is not provided then content will be blocked.
Summary
Description
Rule summary
Protect outgoing HTTP content when the following conditions are met:
the posted data is tagged or classified as any of: 'INFO CBI', 'office', 'partage conter
When this rule is applied perform the following actions: Notify User (Online/Offline), Me
This rule is assigned in 'Groupe d'affectation d'utilisateurs'.
Cancel
< Back
Next >
Finish

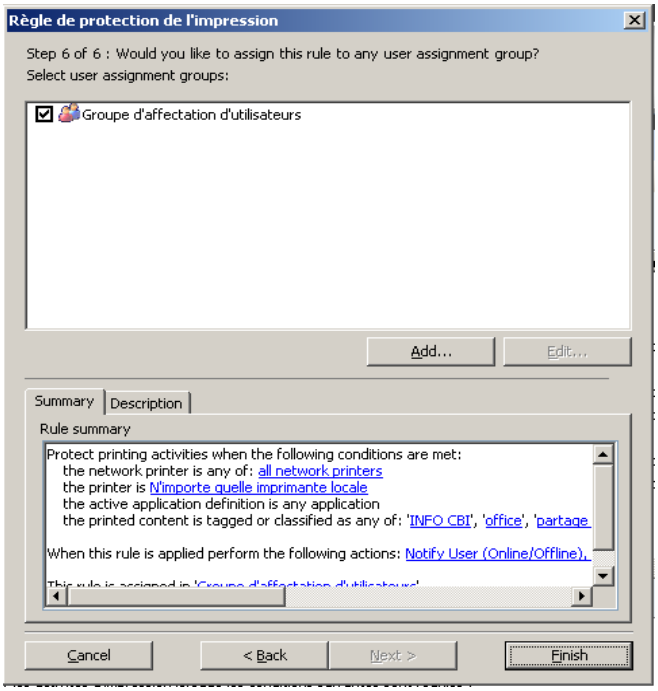

Règle de protection de la publication web
Step 8 of 8 : Would you like to assign this rule to any user assignment group?
Select user assignment groups:
Groupe d'affectation d'utilisateurs
Add...
Edit...
Summary
Description
Rule summary
Protect outgoing HTTP content when the following conditions are met:
the posted data is tagged or classified as any of: 'INFO CBI', 'office', 'partage conter
When this rule is applied perform the following actions: Notify User (Online/Offline), Me
This rule is assigned in 'Groupe d'affectation d'utilisateurs'.
Cancel
< Back
Next >
Finish

. Règle de protection de l'impression

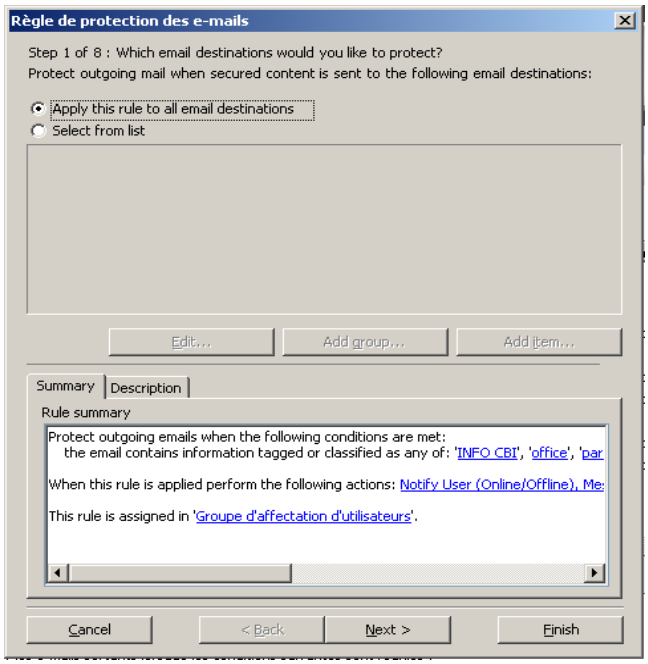


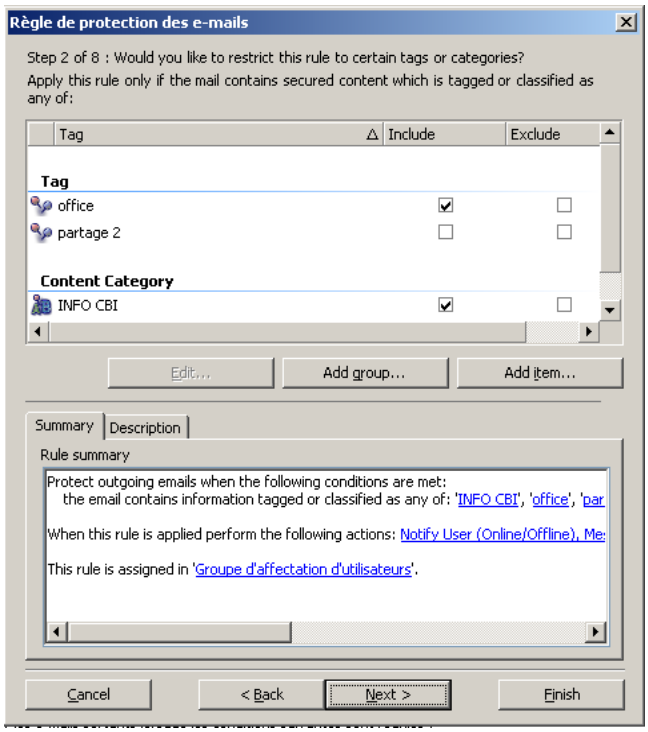


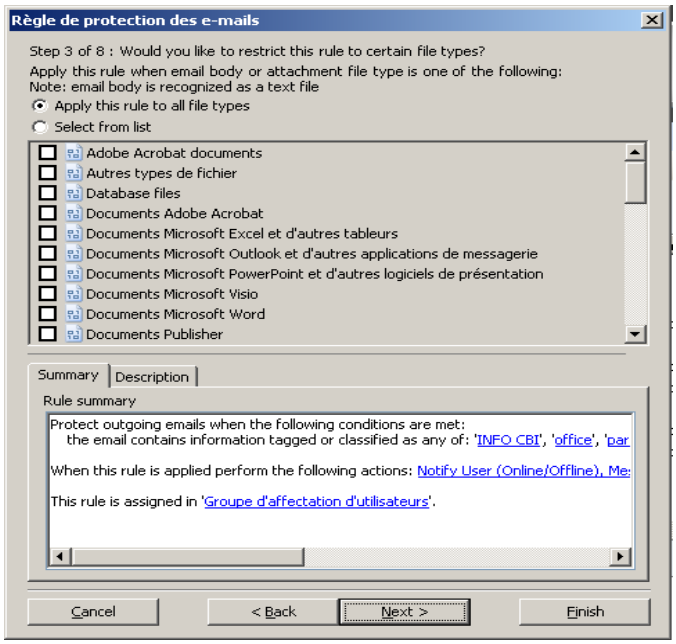


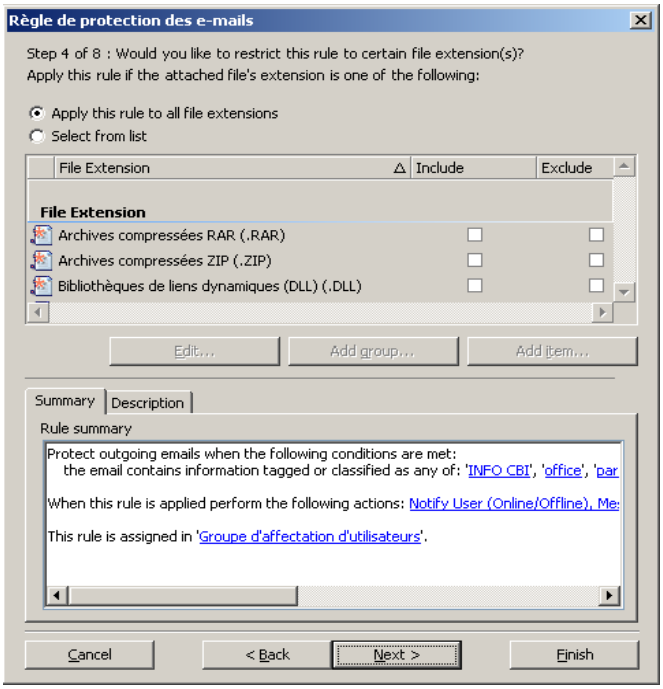


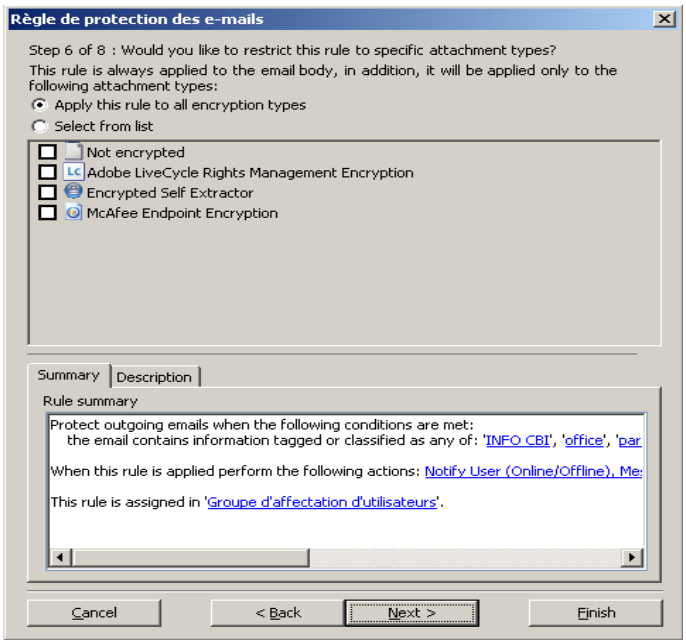
. Règle de protection Email

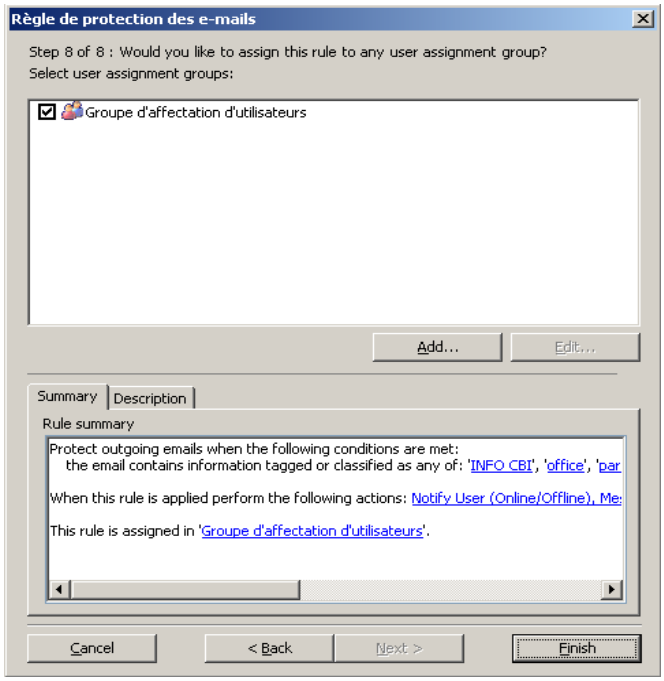


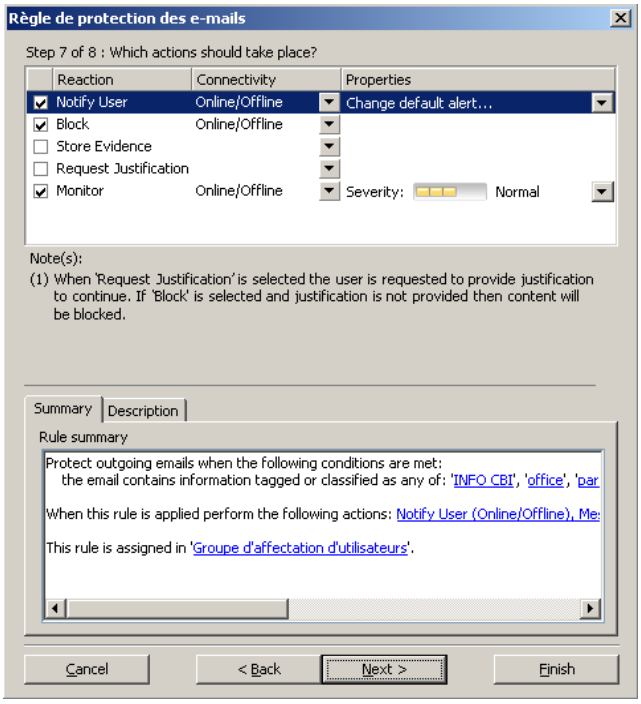




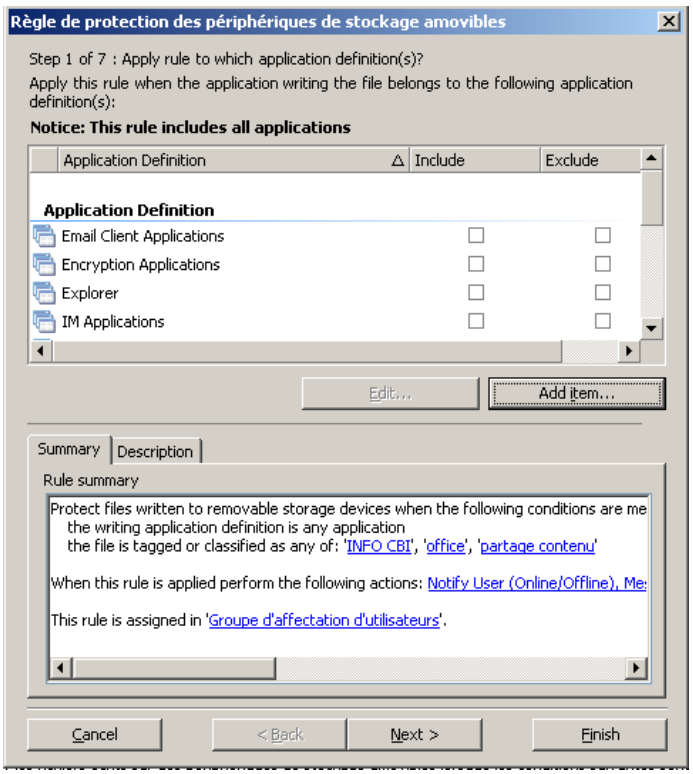


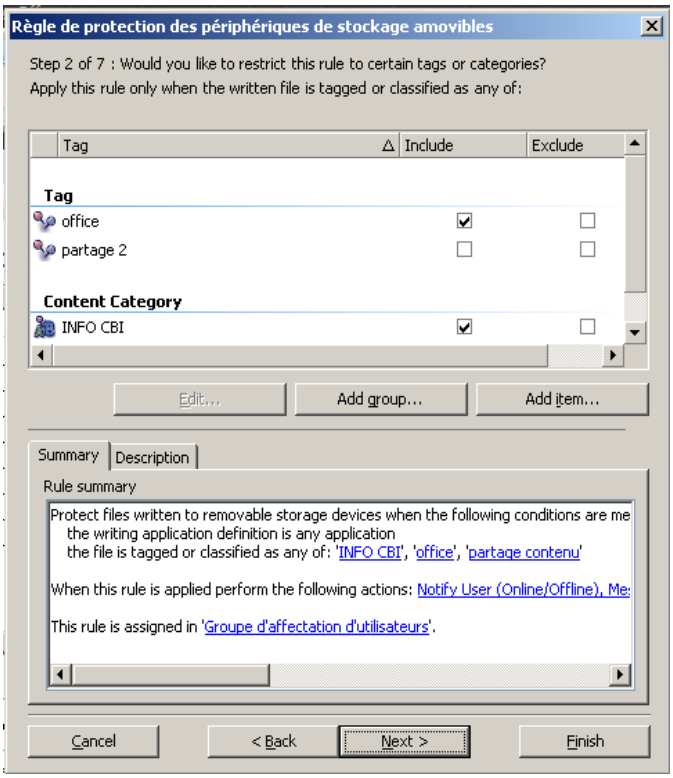

Règle de protection des e-mails
Step 6 of 8 : Would you like to restrict this rule to specific attachment types?
This rule is always applied to the email body, in addition, it will be applied only to the following attachment types:
Apply this rule to all encryption types
Select from list
Not encrypted
Adobe LiveCycle Rights Management Encryption
Encrypted Self Extractor
McAfee Endpoint Encryption
Summary
Description
Rule summary
Protect outgoing emails when the following conditions are met:
the email contains information tagged or classified as any of: 'INFO CBI', 'office', 'par
When this rule is applied perform the following actions: Notify User (Online/Offline), Me:
This rule is assigned in 'Groupe d'affectation d'utilisateurs'.
Cancel
< Back
Next >
Finish

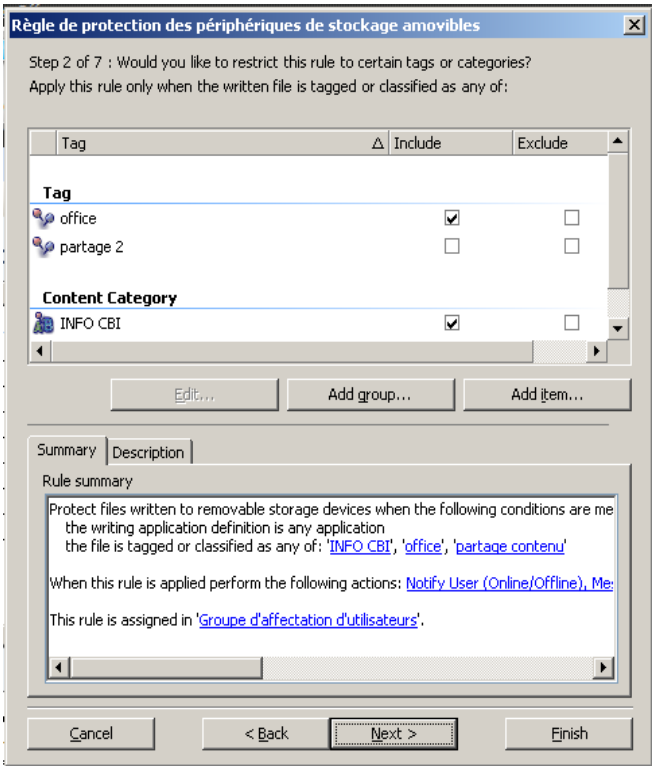

Règle de protection des e-mails
Step 8 of 8 : Would you like to assign this rule to any user assignment group?
Select user assignment groups:
Groupe d'affectation d'utilisateurs
Add...
Edit...
Summary
Description
Rule summary
Protect outgoing emails when the following conditions are met:
the email contains information tagged or classified as any of: 'INFO CBI', 'office', 'par
When this rule is applied perform the following actions: Notify User (Online/Offline), Me:
This rule is assigned in 'Groupe d'affectation d'utilisateurs'.
Cancel
< Back
Next >
Finish

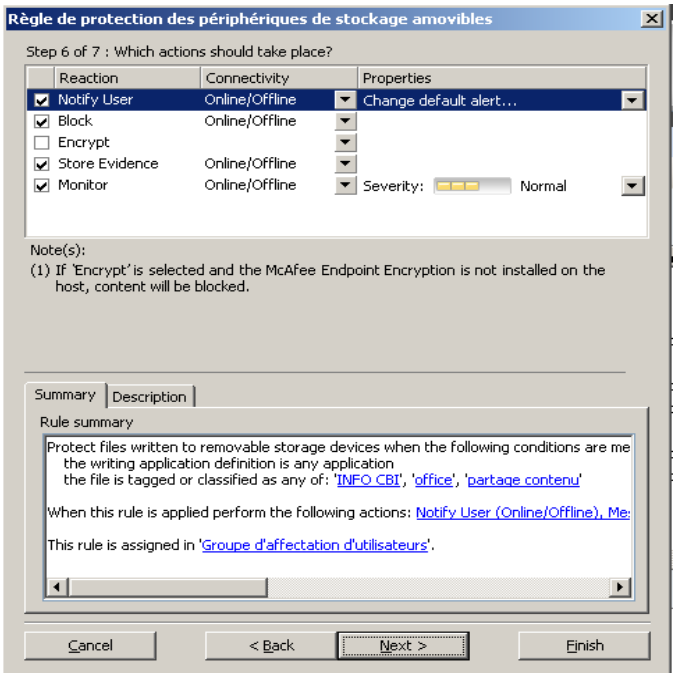

Règle de protection des e-mails
Step 7 of 8 : Which actions should take place?
Reaction
Connectivity
Properties
Notify User
Online/Offline
Change default alert...
Block
Online/Offline
Store Evidence
Request Justification
Monitor
Online/Offline
Severity:
Normal
Note(s):
(1) When 'Request Justification' is selected the user is requested to provide justification to continue. If 'Block' is selected and justification is not provided then content will be blocked.
Summary
Description
Rule summary
Protect outgoing emails when the following conditions are met:
the email contains information tagged or classified as any of: 'INFO CBI', 'office', 'par
When this rule is applied perform the following actions: Notify User (Online/Offline), Me:
This rule is assigned in 'Groupe d'affectation d'utilisateurs'.
Cancel
< Back
Next >
Finish

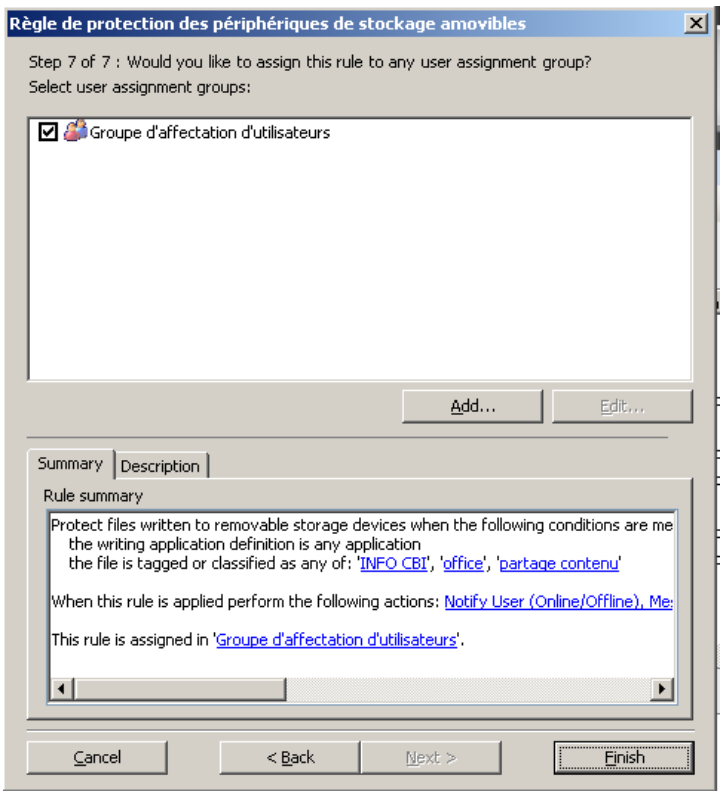
. Règle de protection disque amovible











5 . Rôle du moniteur Host DLP

La surveillance du système consiste à rassembler et à analyser des preuves et des événements, puis à produire des rapports. Le moniteur Host DLP fournit les commentaires nécessaires à la conception d'un système efficace de prévention des fuites de données. L'analyse des preuves et des événements enregistrés permet de déterminer si les règles sont trop restrictives, entraînant des retards inutiles, ou au contraire trop laxistes, favorisant la fuite des données.

Lorsqu'un agent détecte une violation de stratégie, il génère un événement qu'il envoie à l'analyseur d'événements ePO. Ces événements peuvent être visualisés, filtrés et triés dans le moniteur Host DLP, ce qui permet aux administrateurs ou aux responsables de la sécurité de consulter ces événements et de réagir dans les plus brefs délais. Le cas échéant, le contenu suspect est joint à l'événement en tant que preuve.
Dans certain cas il est nécessaire de limiter la quantité d'informations affichées pour pouvoir se concentrer sur les détails importants pour cela on appliquer un filtre pour définir des critères spécifiques et limiter la liste d'événements aux données véritablement significatives, par exemple des événements critiques, Infractions à une nouvelle règle, des événements associés à un utilisateur ou à un ordinateur spécifique.

McAfee Host Data Loss Prevention jouant un rôle majeur dans les mesures prises par une entreprise pour respecter ses obligations réglementaires et la législation en matière de

confidentialité, le moniteur Host DLP présente les informations relatives à la transmission des données sensibles de la façon la plus souple et précise possible.

6 . Administration de la base de données et génération de rapports

La solution McAfee Host Data Loss Prevention est dotée de fonctionnalités intégrées permettant de gérer la base de données et de générer des rapports. Les fonctionnalités de la base de données permettent de supprimer des données dont l'entreprise n'a plus besoin et d'afficher les statistiques de la base de données.

Elle emploie des fonctions de génération de rapports d'ePolicy Orchestrator. Deux types de rapports sont pris en charge :

- Rapports des propriétés DLP
- Rapports des événements DLP

Les rapports des propriétés DLP apparaissent dans DLP :
. Tableaux de bord Résumé des états. Onze requêtes d'événements prédéfinies sont fournies. On trouvera l'ensemble de ces vingt requêtes dans la console d'ePolicy Orchestrator, sous **Menu | Requêtes | Groupes partagés**.

Donc McAfee Host data loss prevention représente un outil très poussée dans le domaine de la prevention contre la fuite de données grâce a ses différentes composants allons de la classification de contenu sensible avec utilisation des dictionnaires, La fonction de documents enregistrés et celle du model textuel au moyen de deux mécanismes: les marqueurs et les catégories de contenu, passant par application des règles de protection qui englobe tout les canaux susceptibles de produire un risque de fuite a titre d'exemple : communication web , email , des supports amovibles, l'impression. Finissant par un système de surveillance qui consiste à rassembler et à analyser des preuves et des événements, afin de produire des rapports qui servant un moyen de vérification de bon fonctionnement des stratégies.

7. Conclusion

La classification des informations de l'entreprise en différentes catégories de Data Loss Prevention constitue une étape primordiale dans le déploiement et l'administration du logiciel McAfee Host Data Loss Prevention. Même s'il existe des principes généraux et des meilleures pratiques, le schéma idéal dépend des objectifs et des besoins spécifiques des entreprises ; il est donc unique pour chaque installation. Mais d'une manière générale pour garantir la protection des données, les entreprises devront observez les principes suivants :

Rapport-Gratuit.com

- Classification les informations à protéger.
- Création des marqueurs ou catégories de contenu pour chaque classification de données.
- Création des règles de marquage et de classification associant les données sensibles aux marqueurs et catégories de contenu appropriés.
- Définition des règles de protection intégrant les marqueurs et les catégories de contenu qui bloquent, surveillent ou chiffrent les données sensibles lors de leur envoi par les utilisateurs vers des périphériques portables ou des emplacements réseau spécifiés.

Conclusion

A l'ère de l'information, «prévenir les pertes» n'est plus limité à la réduction des malversations dans la chaîne d'approvisionnement, le commerce ou l'administration. Désormais, le savoir-faire d'une entreprise se trouve surtout dans des bases de données, emails ou fichiers et non dans des caisses en cartons, entrepôts ou classeurs. Depuis les listes clients, les factures, les déclarations financières jusqu'aux produits et projets d'ingénierie, les organes vitaux d'une entreprise résident autant dans les données électroniques, les réseaux informatiques et les ordinateurs portables dans les bureaux, magasins, usines. Enfermer l'information est impossible ; sa valeur ajoutée repose sur sa facilité d'utilisation à travers toute l'entreprise.

La solution McAfee Data Loss Prevention permet de surveiller et de prévenir les comportements à risques susceptibles d'entrainer des divulgations de données sensibles. Cette protection s'étend aux applications, aux périphériques de stockages amovibles et aux réseaux ; que l'employé en possession des données soit sur son lieu de travail, à son domicile ou en déplacement. L'intégration avec la plateforme McAfee ePolicy Orchestrator offre une gestion centralisée permettant de définir et de gérer les stratégies de protection des données (analyse, audit, déploiements, mises à jour, rapports de conformité).

Grâce à une étude détaillée sur le principe de data loss prevention a compagne par une étude comparative entre les différentes solutions DLP, j'ai pu aborder avec une grande maîtrise la partie pratique de mon projet à savoir, la réalisation d'une maquette de test de la solution McAfee Host Data Loss Prevention.

En termes de perspectives, ce projet peut être par la suite complété par l'intégration de module de cryptage McAfee Endpoint Encryption qui offre des fonctionnalités de chiffrement et de contrôle de l'accès ultraperformantes afin d'empêcher tout accès non autorisé aux données sensibles et de prévenir les fuites et les divulgations de données.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

Caractéristiques de différentes solutions Data Loss Prevention

Produit	strengths	Cautions
CA	. Bonnes fonctions de point final et de découverte et réseau .Une vision progressiste, y compris la gestion des informations de sécurité et d'événement (SIEM), et les offres de gestion d'identité et (IAM) d'accès. .une portée mondiale, faisant appel à de grandes entreprises géographiquement diversifiée.	.En 2009, CA fera face à des chalenges pour comprendre et soutenir le marché de DLP d'entreprise au delà de la base installée traditionnelle d'Orchestria dans des services financiers tout en s'exécutant sur une plus large vision de CA pour intégrer le DLP de CA avec IAM et SIEM
Code Green Networks	.Il a les capacités de réseau et de bonnes fonctions de base de ligne de la découverte, avec une attention particulière sur la facilité d'utilisation et une expérience éprouvée avec les petites entreprises (plus de 2.500 utilisateurs) .Il a intégré l'agent de transfert des messages (MTA) et la fonctionnalité native flexible e-mail via l'intégration des fonctions de chiffrement de Cisco / IronPort Systems, ainsi que la tension de sécurité de technologie dans le produit. Cela ajoute une valeur significative pour les PME, qui préfèrent généralement des solutions intégrées	.son agent point final n'a pas les caractéristiques concurrentielles, telles que le blocage .Il n'a pas d'antécédents de déploiements de grande entreprise. • Ses capacités de recherche sont de portée limitée et de soutien.
Fidelis Security Systems	. offre qui répond aux besoins des grandes entreprises à la recherche des capacités réseau	.Il est précisé que l'intention d'offrir network DLP réduit appel de la société à des organisations à la recherche d'un ensemble de fonctions DLP.
Fidelis Security Systems	. offre qui répond aux besoins des grandes entreprises à la recherche des capacités réseau	.Il est précisé que l'intention d'offrir network DLP réduit appel de la société à des organisations à la recherche d'un ensemble de fonctions DLP.
GTB Technologies	Il dispose d'un réseau équilibré, la découverte et le portefeuille de point de terminaison, avec un bon prix pour les petites organisations. concentrer sur les petites et moyenne entreprises dans les services financiers	ses capacités point finales DLP sont limitées au contrôle de transfert de données vers des supports amovibles.
McAfee	.une présence mondiale, avec un solide réseau de revendeurs à valeur ajoutée, qui fait appel à de grandes entreprises distribuées géographiquement .offre une forte valeur pour les utilisateurs de l'entreprise actuelle de solutions de McAfee .technologie point final et de l'infrastructure réseau (pare-feu passerelle e-mailWeb et IPsec) sont toutes gérées par ses ePolicy (ePO) Orchestrator, ce qui peut réduire le coût de déploiement pour les clients existants McAfee	.Son réseau distinct, point final et de produits de découverte de données ne sont pas complètement intégrés avec l'offre de base de McAfee ePO. .il ya un manque persistant d'intégration entre les points finals sensibles au contenu, de réseau et les capacités de découverte, notamment à l'appui de la gestion centralisée.
Palisade Systems	.la détection de contenus non-anglophones. Bien que Palisade a des clients en dehors de l'Amérique du Nord, son courant principal objectif de vente continue d'être en Amérique du Nord	.Sa feuille de route suit le marché des grandes entreprises, ce qui limite l'appel de la solution pour les PME avec des exigences minimales

RSA, The Security Division of EMC	.Elle a de fortes capacités décrites de contenu possible par des processus d'ingénierie de la connaissance formelle, offrant une vaste gamme de capacités d'inspection DLP. .Son rayonnement mondial fera appel à divers clients géographiquement	.Il est le plus connu pour les solutions DLP réseau et de découverte, avec une offre de point final qui continuera à être contestée les fournisseurs d'antivirus
Symantec	.Il a conduit l'industrie des réseaux et des capacités de flux de travail, équilibrée par la découverte de la concurrence et les capacités des terminaux. sa présence mondiale, avec un réseau de VAR forte, fera appel à de grandes entreprises, réparties géographiquement.	Vontu 9 Agent point final (sorti en Décembre 2008) est plus compétitif que les versions précédentes. .Il a la plus chère la totalité des coûts de licence Enterprise Suite. .Sa console d'administration n'est pas localisée, ce qui peut entraver les scénarios de déploiement dans des environnements non-anglophones
Trend Micro	Elle a de fortes capacités de point final.	.Son produit de point final a besoin d'améliorations au contenu de sensibilisation et de blocage. Sa perte de partenaires DLP sensibles au contenu (Reconnex, acquis par McAfee, et Utimaco, acquise par Sophos) affecte négativement sa compétitivité
Verdasys	.Sa solution est séduisante pour les entreprises qui nécessitent des contrôles rigoureux pour la protection de la propriété intellectuelle.	.Son prix élevé se traduira par une perte de compétitivité
Websense	Sa présence mondiale, avec un réseau diversifié de revendeurs à valeur ajoutée, fait appel à de grandes entreprises, réparties géographiquement.	Il a une offre qui est le plus attirant pour les clients Websense actuels qui souhaitent tirer parti de produits déjà déployés
Vericept	capacités réseau, la découverte et critère d'évaluation des DLP, ainsi que bon workflow. utilisation du contenu des descriptions de l'analyse linguistique (CANDL) offre d'appel important pour les entreprises qui souhaitent inscrire un contenu unique et très spécifique pour l'inspection DLP	Il a un minimum de localisation et de support des caractères à double octet, ce qui limite son appel pour les grandes entreprises et des marchés internationaux

Bibliographie

- http://www.mcafee.com/fr/enterprise/products/data_protection/index.html

- Understanding and Selecting a Data Loss Prevention Solution : Securosis, L.L.C.

- Data Loss Prevention Program : Powell Hamilton Managing Consultant Foundstone Professional Services
- McAfee Data Loss Prevention : Best Practices Guide
- McAfee Host Data Loss Prevention 9.0 Installation Guide for ePolicy Orchestrator 4.5
- Release Notes for McAfee Host Data Loss Prevention 9.0.0
- Livre blanc RSA Six bonnes pratiques de prévention des pertes de données
- McAfee ePolicy Orchestrator 4.5 Evaluation Guide
- McAfee ePolicy Orchestrator 4.5 Installation Guide
- McAfee ePolicy Orchestrator 4.5 Product Guide
- McAfee Host Data Loss Prevention 9.0 for ePolicy Orchestrator 4.5 Product Guide
- Magic Quadrant for Content-Aware Data Loss Prevention
- The_Forrester_Wave_DataLeakPrevention_Q2_2008