
Microsoft® Forefront™

Produits de sécurité pour les entreprises

Microsoft Corporation

Date de publication : septembre 2006

Résumé

Microsoft® Forefront™ regroupe une gamme complète de produits de sécurité pour les entreprises qui souhaitent une plus grande protection et un meilleur contrôle de la sécurité de leur infrastructure réseau. Les produits Forefront s'intègrent aisément entre eux, mais également à l'infrastructure informatique d'une entreprise. En outre, en les conjuguant à d'autres solutions tierces compatibles, il devient possible de mettre en œuvre une stratégie de défense en profondeur encore plus élaborée, de bout en bout. Des fonctions simplifiées d'administration, de création de rapports, d'analyse et de déploiement permettent aux administrateurs de protéger de manière plus efficace les informations de leur entreprise, tout en sécurisant les accès aux applications et aux serveurs. Avec Microsoft Forefront, les entreprises sont armées pour mieux résister aux menaces en constante évolution et répondre aux exigences toujours croissantes du marché.

Microsoft®

Les informations contenues dans ce document représentent l'opinion actuelle de Microsoft Corporation sur les points cités à la date de publication. Microsoft s'adapte aux conditions fluctuantes du marché et cette opinion ne doit pas être interprétée comme un engagement de la part de Microsoft ; de plus, Microsoft ne peut pas garantir la véracité de toute information présentée après la date de publication.

Ce document est fourni uniquement à titre indicatif. MICROSOFT EXCLUT TOUTE GARANTIE, EXPRESSE OU IMPLICITE, EN CE QUI CONCERNE LES INFORMATIONS DE CE DOCUMENT.

L'utilisateur est tenu de respecter la réglementation relative aux droits d'auteur applicable dans son pays. Sans restriction des droits dérivés des droits d'auteur, aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de restitution, ou transmise à quelque fin, par quelque moyen (électronique, mécanique, photocopie, enregistrement ou autre) ou dans quelque but que ce soit sans la permission expresse et écrite de Microsoft Corporation.

Microsoft peut détenir des brevets, avoir déposé des demandes d'enregistrement de brevets ou être titulaire de marques, droits d'auteur ou autres droits de propriété intellectuelle portant sur des éléments qui font l'objet du présent document. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture de ce document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

© 2006 Microsoft Corporation. Tous droits réservés.

Microsoft, Active Directory, Forefront, Visual Studio, Windows, Vista, Longhorn, le logo Windows et Windows Server sont soit des marques déposées, soit des marques de fabrique de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Toutes les autres marques déposées appartiennent à leurs propriétaires respectifs

Table des matières

Connectivité à grande échelle	2
Menaces en perpétuelle évolution	2
Solutions disparates.....	2
Difficultés opérationnelles	3
Principes de conception.....	4
Solution complète.....	4
Solution intégrée	5
Solution simplifiée	5
Gamme de produits Forefront	7
Protection et contrôle de l'accès à la périphérie du réseau	8
Microsoft Internet Security and Acceleration Server 2006 (ISA Server 2006).....	8
Whale Communications Intelligent Application Gateway	8
Protection des serveurs d'applications	9
Microsoft Forefront Security pour Exchange Server	9
Microsoft Forefront Security pour SharePoint.....	9
Microsoft Forefront Security pour Office Communications Server.....	9
Protection des systèmes d'exploitation clients et serveurs	10
Microsoft Forefront Client Security.....	10
Systèmes d'exploitation	12
Protection d'accès réseau (NAP).....	12
Protection des informations.....	13
Services	13
Gestion des identités	14
Gestion des systèmes.....	14
Outils de développeurs	14
Systèmes d'exploitation	18
Protection d'accès réseau (NAP).....	18
Services	18
Protection des informations.....	18
Gestion des identités	18

Gestion des systèmes.....	18
Outils de développeur et conseils.....	18

Introduction

Au cours de ces dix dernières années, Internet est devenu une ressource essentielle pour les entreprises de toute taille. Employés, partenaires, fournisseurs et clients sont en mesure de communiquer plus efficacement et d'obtenir des informations à tout moment, depuis n'importe quel endroit. Grâce à des processus simplifiés et des sites en libre service, ils peuvent en outre économiser du temps et de l'argent.

Malgré ses nombreux avantages, il n'en demeure pas moins qu'Internet est aussi à l'origine d'une multitude de défis pour les entreprises. Les services d'informations dynamiques, capables de générer des informations personnalisées, ont également donné naissance à des problèmes liés à la confidentialité et aux réglementations qui en découlent. La connectivité qui a permis d'améliorer l'efficacité des entreprises a aussi facilité la tâche aux utilisateurs mal intentionnés. Les réseaux des entreprises et leurs informations sensibles sont désormais la cible d'attaques malveillantes et de tentative d'accès non autorisées. En outre, au fil des années, les menaces sont de plus en plus sophistiquées et dangereuses.

Face à ces menaces en constante évolution, la gestion de la sécurité des réseaux s'avère être une tâche complexe, requérant fréquemment l'intégration et la sécurisation de nombreuses technologies, afin de garantir à la fois une facilité d'accès et une sécurité à toute épreuve. L'utilisation de solutions de sécurité pesantes, imposant un délai inacceptable pour autoriser l'accès aux ressources informatiques, risque d'avoir un impact négatif sur l'efficacité, tandis que l'absence de communications aisées et sécurisées avec clients et partenaires est susceptible d'entraîner la perte d'opportunités commerciales. En revanche, une trop grande ouverture peut mener à la divulgation d'informations confidentielles, à des pertes financières, mettant en péril l'existence même d'une entreprise.

Faisant partie des leaders de l'industrie informatique, Microsoft s'est engagé à fournir des produits plus sûrs et à aider ses clients à les déployer et les gérer de manière efficace. L'une des solutions proposées pour concrétiser cet engagement est Microsoft Forefront, une gamme de produits de sécurité complète pour les entreprises de toute taille. Microsoft Forefront permet aux entreprises d'offrir un accès sécurisé à toute heure et en tout lieu, tout en protégeant leurs informations contre les attaques et les utilisateurs non autorisés.

Défis et tendances liés à la sécurité

Malgré les investissements importants consentis dans le domaine de la sécurité des réseaux et des systèmes informatiques depuis environ quinze ans, les défis liés à la sécurité ne cessent de croître. Actuellement, les entreprises sont exposées à un nombre de plus en plus élevé de menaces, virus, courriers indésirables et attaques visant leurs informations sensibles.

Connectivité à grande échelle

Internet est désormais une ressource essentielle pour les entreprises, quelle que soit leur taille. Ces dernières sont ainsi en mesure de fournir des informations en temps réel aux employés, d'optimiser leurs campagnes de marketing, de réaliser des économies grâce aux solutions de self-service proposées aux clients et de rationaliser les processus à destination des fournisseurs et autres partenaires.

Si les avantages d'une entreprise parfaitement connectée sont nombreux, les défis à relever sont également importants. Cette connectivité à grande échelle a ouvert la porte à une pléthore de menaces en constante évolution, facilitant la tâche aux auteurs d'attaques malveillantes de grande envergure et aux utilisateurs non autorisés tentant d'accéder aux réseaux des entreprises. Ces risques d'attaques sont en outre proportionnels au nombre de partenaires de l'entreprise.

Menaces en perpétuelle évolution

Le domaine de la sécurité des ordinateurs et des réseaux est confronté à une évolution inquiétante des types de menaces de sécurité, ainsi que des motifs sous-jacents. Dans la mesure où les pare-feux traditionnels ne sont pas conçus pour détecter et bloquer les intrusions au niveau de la couche application, la plupart des attaques lancées sur Internet se sont maintenant déplacées vers le haut de la pile des protocoles réseau, ciblant des applications telles que la messagerie électronique, les serveurs Web et les applications de collaboration en ligne.

Les motifs de ces attaques ont également changé ; les pirates sont désormais attirés par l'appât du gain criminel, s'en prenant aux informations confidentielles - extrêmement sensibles - d'entreprises spécifiques : noms, adresses, numéros de sécurité sociale ou données financières. Pour rendre le défi encore plus complexe, les attaques à grande échelle, totalement aléatoires, n'ont pas disparu. Bien au contraire, leur nombre a augmenté de manière exponentielle, avec l'apparition de pirates informatiques néophytes (« script kiddies ») qui se servent d'outils de piratage automatisés pour perpétrer des attaques contre des entreprises de toute taille. À mesure que les attaques augmentent, celles-ci coûtent de plus en plus cher à l'entreprise, augmentent le temps nécessaire pour la réparation et ont un impact négatif sur la productivité et l'exploitation de l'infrastructure informatique.

Solutions disparates

Jusqu'ici, les solutions de sécurité informatique ont mis en œuvre des produits divers émanant de plusieurs fournisseurs, ce qui nécessitait des outils et des infrastructures multiples pour les opérations d'administration, d'analyse et de création de rapports. Le déploiement et la configuration de ces solutions de sécurité complexes peuvent s'avérer laborieux et nécessiter beaucoup de temps. En outre, un trop grand nombre de produits de sécurité offrent un degré peu élevé d'interopérabilité et d'intégration avec l'infrastructure informatique et de sécurité existante. Les solutions résultantes sont

difficiles à gérer, elles représentent un coût total de possession élevé, mais surtout, elles accroissent les risques de failles dans la sécurité du réseau.

Difficultés opérationnelles

Compte tenu de l'importance de la sécurité au sein d'une entreprise, il est essentiel de pouvoir mettre en œuvre une administration efficace et un contrôle de stratégies centralisé. Pourtant, cela s'avère souvent impossible, compte tenu de la nature fragmentée de la majorité des solutions de sécurité. Sans une administration et des outils de rapport centralisés, et la bonne visibilité qu'ils offrent sur la sécurité globale du réseau, le déploiement et l'administration de la sécurité sont souvent difficiles, inefficaces, sources d'erreurs et consommateurs de temps.

Malgré les défis, le besoin d'une administration des stratégies et d'une centralisation des rapports ne s'est jamais tant fait sentir. Cela est particulièrement vrai en raison des exigences complexes en matière de sécurité imposées par les lois Sarbanes-Oxley, HIPAA (Health Insurance Portability and Accountability Act) de 1996 et d'autres réglementations nationales et internationales. Désormais, au vu de ces lois, les entreprises doivent évaluer les implications d'intrusions au niveau de leur réseau et de l'absence d'une infrastructure de sécurité adéquate. Toute entreprise opérant sur Internet doit également prendre en considération les responsabilités qui lui incombent et les risques de poursuites judiciaires, particulièrement dans les domaines touchant la confidentialité, le partage de fichiers, les ressources humaines, la santé et les relations avec les investisseurs. Dans un tel environnement, les utilisateurs malveillants présentent un risque non seulement pour les données, mais également pour les entreprises, qui courent le risque de ne pas pouvoir satisfaire à ces exigences.

Gamme de produits Microsoft Forefront

Microsoft Forefront regroupe une gamme complète de produits de sécurité qui assurent aux entreprises une plus grande protection et renforcent la sécurité de leur infrastructure réseau. Les produits Microsoft Forefront s'intègrent aisément les uns aux autres, mais également à l'infrastructure informatique d'une entreprise déjà en place. En outre, ils peuvent être conjugués à d'autres solutions tierces compatibles, afin d'assurer une stratégie de défense en profondeur encore plus élaborée, d'un bout à l'autre de la chaîne. Des fonctions simplifiées d'administration, de création de rapports, d'analyse et de déploiement permettent de protéger efficacement les informations, tout en sécurisant les accès aux applications et aux serveurs.

Principes de conception

Microsoft a conçu la gamme de produits de sécurité Forefront pour faire face aux défis que représentent la connectivité à grande échelle, les menaces de plus en plus sophistiquées, les solutions éparpillées et les difficultés opérationnelles. Microsoft est persuadé que pour faire face à ces défis, toute solution de sécurité correctement conçue doit être complète, intégrée et simplifiée. Ces trois caractéristiques sont les principes autour desquels s'articulent tous les produits de sécurité de la gamme Forefront.

Solution complète

Les produits Forefront offrent une solution complète garantissant une protection intégrale de l'infrastructure informatique.

- **Protection des systèmes d'exploitation** : Forefront assure la protection des systèmes d'exploitation clients et serveurs Microsoft. Les fonctions de sécurité très réactives de Microsoft Forefront Client Security permettent la détection et la suppression à la demande, selon un planning ou en temps réel, de virus, logiciels espions, rootkits et autres menaces émergentes.
- **Protection d'applications serveurs critiques** : Forefront est conçu pour protéger les serveurs d'applications Microsoft via une stratégie de défense en profondeur. ISA Server 2006 offre un contrôle d'accès robuste ainsi qu'une inspection exhaustive des données des applications et des protocoles. Les produits de sécurité serveur Forefront protègent les applications serveurs spécifiques contre les menaces à l'aide d'une architecture unique qui intègre plusieurs moteurs d'analyse de la sécurité et offre un niveau extrêmement élevé de protection et de fiabilité.
- **Accès contrôlé et sécurisé** : Forefront incorpore de nombreuses technologies de pare-feu, VPN et chiffrement, ainsi que des fonctions de gestion des identités garantissant que seules les personnes dûment autorisées seront en mesure d'accéder aux ressources informatiques et aux données appropriées.
- **Protection des données sensibles** : les produits Forefront protègent les données sensibles et la propriété intellectuelle. ISA Server 2006 combine des filtres spécifiques aux applications du réseau et des technologies qui assurent la confidentialité et l'authenticité des données importantes.

Solution intégrée

Les produits Forefront offrent plusieurs niveaux d'intégration afin que les administrateurs soient en mesure de gérer et de contrôler de manière optimale la sécurité du réseau.

- **Intégration aux applications** : les produits Microsoft Forefront, dont le rôle est de faire barrage aux programmes malveillants et de contrôler et sécuriser les accès réseau, sont spécialement conçus pour protéger et s'intégrer aux applications serveurs clés des entreprises telles que Microsoft Exchange, Outlook® Web Access et SharePoint. Cette intégration offre une protection essentielle contre les nouvelles attaques ciblant plus particulièrement les applications.
- **Intégration à l'infrastructure informatique** : les produits de sécurité fonctionnent de pair avec l'infrastructure informatique déjà en place, notamment les services d'annuaire, les outils d'administration des systèmes et les services de distribution et de mise à jour d'applications logicielles. L'élément clé est une infrastructure unifiée permettant l'administration, en toute transparence, du déploiement, de la distribution, de la configuration et de la mise en œuvre des services de sécurité. En outre, le contrôle de l'ensemble de ces opérations doit être effectué avec un haut degré de granularité.
- **Intégration avec Forefront** : les produits Forefront sont conçus pour fonctionner en parfaite synergie, afin de pouvoir exploiter l'ensemble des fonctionnalités et d'offrir une solution de sécurité optimale.
- **Intégration à d'autres produits** : les produits Forefront protègent et sécurisent les infrastructures Windows. Toutefois, un grand nombre d'entreprises déploient des produits de sécurité tiers et, pour cette raison, la conception des produits Forefront leur permet de mieux s'intégrer à des solutions hétérogènes.

Solution simplifiée

Les produits Forefront sont conçus pour simplifier le déploiement, la configuration, l'administration, la création de rapports et l'analyse afin qu'utilisateurs et administrateurs puissent avoir pleinement confiance dans la protection de leur entreprise.

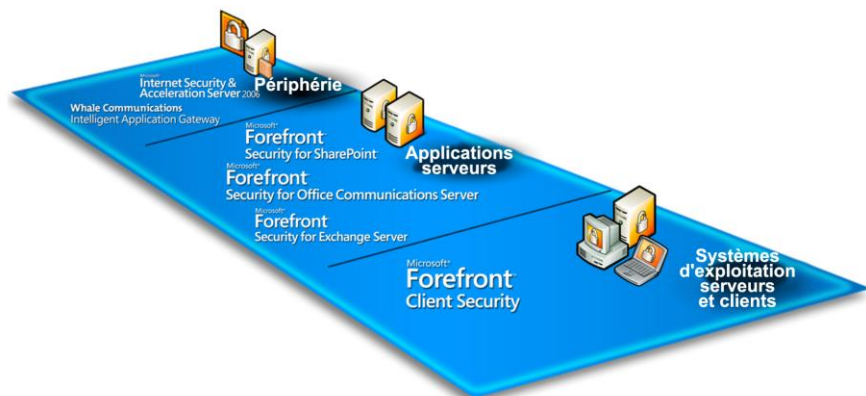
- **Déploiement simplifié** : des utilitaires tels que l'outil d'analyse des meilleures pratiques d'ISA Server et des Assistants de configuration aident à la mise en place de la base solide nécessaire pour une installation de sécurité robuste. Forefront fonctionne avec Active Directory et les systèmes de mise à jour tels que Systems Management Server, afin d'offrir une base commune pour l'administration des modifications et des configurations. Les utilisateurs et les administrateurs tirent parti de la distribution centralisée de configurations et de stratégies, de mises à jour des systèmes d'exploitation et des programmes antivirus pour les hôtes clients et serveurs.
- **Rapports et analyses unifiés** : Forefront centralise la collecte et l'analyse des informations se rapportant à l'administration de la sécurité en stockant l'ensemble des données liées à la sécurité dans un référentiel SQL Server™ unique. À l'aide de SQL Server Reporting and Analysis Services, il peut également identifier et interpréter les événements de sécurité.
- **Administration simplifiée** : Forefront centralise l'administration de la sécurité et les rapports ; ses composants s'intègrent parfaitement aux systèmes d'administration existants, notamment

Microsoft Operations Manager, Microsoft Systems Management Server et Windows Server™ Update Services. Les consoles d'administration intégrées de Forefront offrent aux utilisateurs la convivialité et les interfaces Microsoft avec lesquelles ils sont déjà familiarisés. Il est ainsi possible de réduire le temps de formation et les coûts afférents pour l'entreprise.

Gamme de produits Forefront

Microsoft Forefront¹ regroupe plusieurs produits dont certains assurent une protection et un contrôle d'accès en périphérie, tandis que d'autres protègent les systèmes d'exploitation et les serveurs d'applications Windows de programmes malveillants tels que virus, rootkits et courriers indésirables.

- Microsoft Internet Security and Acceleration Server (ISA Server) 2006
- Whale Communications Intelligent Application Gateway (IAG)
- Forefront Security pour Exchange Server
- Forefront Security pour SharePoint
- Forefront Security pour Office Communications Server
- Forefront Client Security



¹ Microsoft a lancé la marque Forefront le 11 juin 2006. Durant les prochains mois, les noms des produits existants seront modifiés pour refléter leur inclusion dans la marque Forefront. Les nouveaux noms de ISA Server 2006 et Whale IAG n'ont pas encore été finalisés.

Noms des produits	Actuel	2e semestre 2006	2007 et au-delà
Client			Microsoft Forefront Client Security
Server	Microsoft Antigen for Exchange Microsoft Antigen for SMTP Gateways Microsoft Antigen Spam Manager	Microsoft Forefront Security for Exchange Server	
	Antigen for SharePoint	Microsoft Forefront Security for SharePoint	
	Antigen for Instant Messaging	Microsoft Forefront Security for Office Communications Server	
Périphérie	Microsoft Internet Security & Acceleration Server 2007 Whale Communications Intelligent Application Gateway		à définir à définir

Cette gamme complète de produits permet de protéger les données et de contrôler l'accès à un ensemble de systèmes d'exploitation, d'applications et de serveurs, aidant ainsi les entreprises à renforcer leur ligne de défense contre les menaces, en constante évolution.

Protection et contrôle de l'accès à la périphérie du réseau

Microsoft Internet Security and Acceleration Server 2006 (ISA Server 2006)

Whale Communications Intelligent Application Gateway

Les réseaux des entreprises doivent contrecarrer un nombre toujours croissant d'attaques de plus en plus ciblées et sophistiquées. Si la protection des ressources au niveau du siège de l'entreprise et de ses filiales permet un accès en toute transparence aux fonctions d'entreprise légitimes, celle-ci requiert néanmoins une passerelle de périphérie sophistiquée et multifonction, capable de combattre les attaques de plus en plus nombreuses et sophistiquées à l'encontre des applications.

Microsoft
**Internet Security &
 Acceleration Server 2006**
Whale Communications
 Intelligent Application Gateway

ISA Server 2006 est une passerelle de sécurité intégrée, destinée à protéger les environnements informatiques contre les attaques provenant d'Internet, tout en permettant aux utilisateurs d'accéder rapidement et de manière sécurisée aux applications et aux données. ISA Server 2006 prend en compte trois scénarios de déploiement principaux :

- La publication par les entreprises d'applications sécurisées à l'aide d'ISA Server 2006 permet à des utilisateurs distants, situés hors du réseau de l'entreprise, d'accéder de façon sécurisée à des applications telles que Exchange, SharePoint ou d'autres serveurs d'applications Web.
- Les entreprises peuvent utiliser ISA Server 2006 en tant que passerelle, afin de permettre à leurs filiales de bénéficier d'une connectivité sécurisée, tout en exploitant la bande passante réseau de manière optimale.
- La protection de l'accès Web à l'aide d'ISA Server 2006 permet aux entreprises de protéger leur environnement contre les menaces internes et externes en provenance d'Internet.

ISA Server 2006 examine le trafic réseau au niveau de la couche application, plutôt que de se limiter aux en-têtes des paquets réseau. Il vérifie en détail le contenu des paquets afin de déterminer si ces derniers sont conformes aux attentes des applications. Seuls les paquets conformes sont ensuite acheminés vers les serveurs, ce qui permet de bloquer les attaques malveillantes activées par des paquets mal formés. ISA Server est également doté de fonctions d'inspection de contenu de paquets chiffrés lui permettant d'interrompre les connexions SSL entrantes, puis de rechiffrer les paquets valides avant de les acheminer.

Outre ISA Server 2006, les entreprises peuvent également mettre en œuvre la solution IAG (Intelligent Application Gateway) de Whale Communications. La solution Intelligent Application Gateway de Whale Communications, récemment acquise par Microsoft, protège les applications Web et VPN SSL, ce qui ouvre l'accès à une vaste gamme d'applications réseau à partir de périphériques gérés et non gérés. La solution IAG propose des capacités d'accès sophistiquées, basées sur ses fonctionnalités VPN SSL :

- **VPN SSL** : la technologie VPN SSL permet la connectivité à grande échelle, l'accès, l'authentification utilisateur basée sur les stratégies et les autorisations, à partir d'une vaste gamme de périphériques et d'emplacements.
- **Sécurité des points terminaux** : elle applique des stratégies très précises au niveau du navigateur et permet de vérifier la conformité des points terminaux et la sécurité des sessions par le biais de fonctions intégrées de sécurité et de contrôle d'accès des points terminaux, tels que le nettoyeur de cache Whale Attachment Wiper.
- **Optimisation d'applications** : modules logiciels qui ajoutent des fonctions d'inspection de contenu et de stratégies personnalisées aux applications Microsoft, aux systèmes de planification de ressources d'entreprise (ERP) et de gestion de la relation client (CRM) ainsi qu'aux plates-formes de collaboration tiers. Les clients disposant d'applications métiers personnalisées peuvent avoir recours à l'outil Optimizer Toolkit pour configurer IAG pour des besoins de stratégie et de sécurité spécifiques. Microsoft entend poursuivre ses investissements et son engagement vis à vis de cette technologie, particulièrement l'optimisation des applications Microsoft et des applications tierces.

Protection des serveurs d'applications

Microsoft Forefront Security pour Exchange Server

Microsoft Forefront Security pour SharePoint

Microsoft Forefront Security pour Office Communications Server

Microsoft Forefront renforce la protection des serveurs de messagerie et de collaboration Microsoft des entreprises contre les virus, les vers, les courriers indésirables et autres contenus inappropriés avant qu'ils ne puissent affecter les entreprises et les utilisateurs. Parmi ces serveurs d'applications figurent notamment Exchange Server, des passerelles SMTP (Simple Mail Transfer Protocol) Windows, Microsoft Office Communications Server et Microsoft Windows SharePoint Services. Les avantages qu'offre Forefront pour la sécurité des applications serveurs sont notamment :

- **Protection avancée** : plusieurs moteurs d'analyses, opérant à plusieurs niveaux de l'infrastructure de messagerie, renforcent la protection contre les menaces.
- **Disponibilité et contrôle** : une parfaite intégration avec les serveurs Microsoft optimise le contrôle de la disponibilité et de l'administration.
- **Contenu sécurisé** : permet aux entreprises d'éliminer tout langage inapproprié ou pièces jointes dangereuses des communications internes et externes.

Grâce à une approche unique, faisant appel à plusieurs moteurs d'analyse, les produits de sécurité de serveur Forefront offrent une protection réellement inégalée contre les programmes malveillants. Le concept de la défense à plusieurs niveaux est depuis longtemps un élément clé de la sécurité des entreprises. Il part du principe qu'une attaque parvenant à s'infiltrer au-delà d'un niveau de protection, sera bloquée à un niveau ultérieur. Forefront a appliqué ce concept au domaine de la protection

Microsoft®
Forefront
Security for Exchange Server

Microsoft®
Forefront
Security for SharePoint

Microsoft®
Forefront
Security for Office Communications Server

contre les programmes malveillants. Si un moteur d'analyse ne parvient pas à identifier un virus spécifique, il est improbable que le virus parvienne à contourner plusieurs moteurs antivirus, développés par divers chercheurs de virus et plusieurs sociétés utilisant des technologies différentes. Forefront utilise ce type de défense à plusieurs niveaux en administrant, de manière intelligente, jusqu'à 9² moteurs antivirus, parmi les plus performants dans le domaine, au sein d'une même solution. Chacun de ces moteurs a ses points forts spécifiques ; par exemple, certains excellent dans la détection de vers, tandis que d'autres moteurs offrent de meilleures performances lorsqu'il s'agit d'identifier des chevaux de Troie. Forefront tire parti de ces spécificités en combinant plusieurs des moteurs antivirus les plus performants sur le marché au sein d'un même produit, offrant une fiabilité et une protection globales encore plus grandes³. Dans la mesure où une entreprise n'a plus à acheter et à déployer de nombreux produits antivirus, elle peut profiter de la solution avantageuse que représentent plusieurs moteurs regroupés au sein d'une même solution.

La sécurité de serveur Forefront permet ainsi aux entreprises de tirer pleinement parti d'une solution unique, incorporant plusieurs moteurs, sans devoir acheter et déployer de nombreux produits antivirus.

Protection des systèmes d'exploitation clients et serveurs

Microsoft Forefront Client Security

Facile à prendre en main et à administrer à partir d'un emplacement centralisé, Forefront Client Security protège de manière homogène les ordinateurs de bureau, les ordinateurs portables et les systèmes d'exploitation serveur des entreprises contre les programmes malveillants. Basé sur la technologie de protection de Microsoft qui a déjà fait ses preuves et a été adoptée par des millions d'utilisateurs à travers le monde, Forefront Client Security assure une protection contre les menaces émergentes telles que les logiciels espions et les rootkits, mais également les menaces traditionnelles telles que les virus, les vers et les chevaux de Troie.



Grâce à une administration centralisée simplifiée et une meilleure visibilité des menaces et des failles, Forefront Client Security aide les entreprises à se protéger sereinement et de manière plus efficace. Forefront Client Security s'intègre aux infrastructures déjà en place, comme Active Directory, et complète les autres technologies de sécurité Microsoft afin d'offrir une plus grande protection et un meilleur contrôle.

Les avantages de Microsoft Forefront Client Security sont notamment :

- **Protection unifiée** : Forefront Client Security offre une protection unifiée contre les programmes malveillants actuels et émergents, garantissant aux administrateurs et aux utilisateurs une meilleure protection de leurs systèmes d'informations face à une vaste gamme de menaces.

² Les moteurs disponibles sont ceux de Microsoft, CA InoculateIT, CA Vet, Norman, Sophos, Authentium, Kaspersky, VirusBuster et AhnLab.

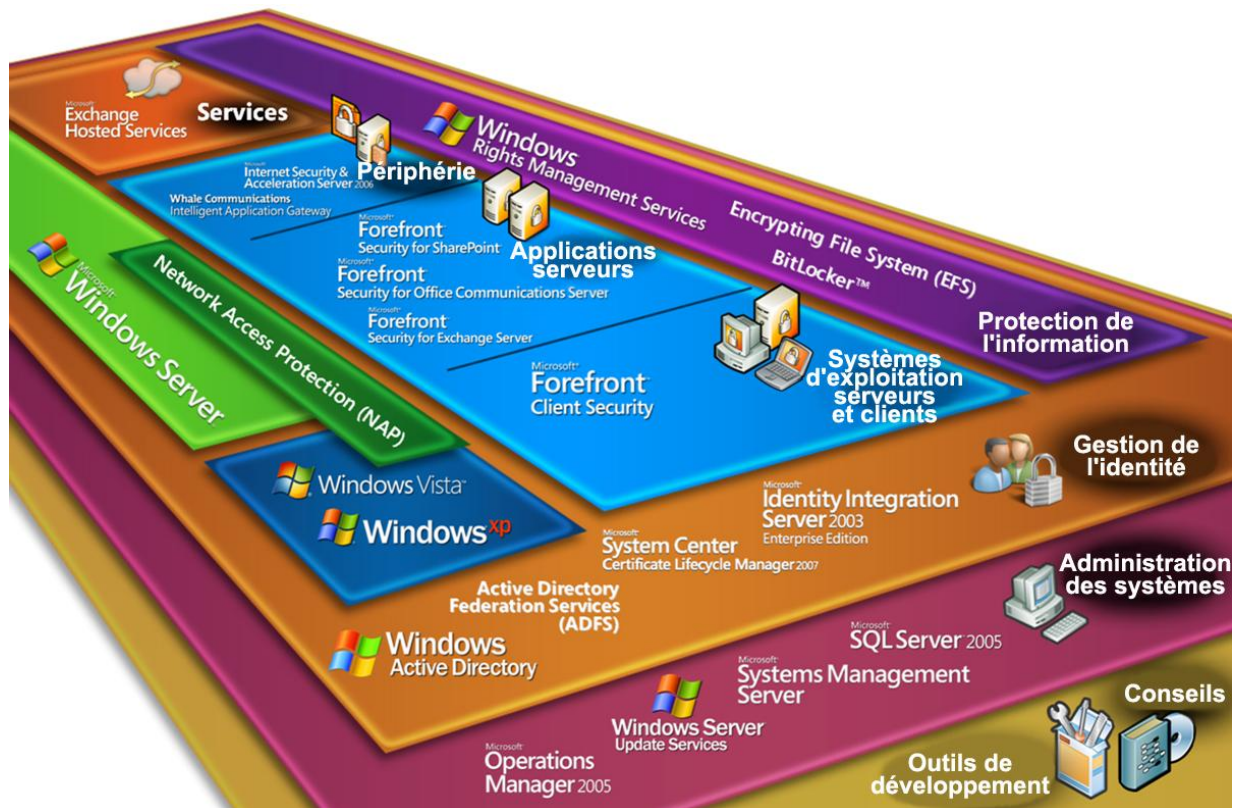
³ Microsoft recommande de ne pas activer plus de cinq moteurs dans une installation de produit donnée. Cette méthode permet d'obtenir à la fois la meilleure protection et les meilleures performances possibles.

- **Administration simplifiée** : Forefront Client Security facilite l'administration en la centralisant. Les entreprises sont ainsi protégées avec un maximum d'efficacité.
- **Visibilité et contrôle renforcés** : Forefront Client Security génère des rapports de sécurité détaillés et hiérarchisés, ainsi qu'un cliché instantané au niveau du tableau de bord. Ainsi, les entreprises disposent d'une grande visibilité et d'un meilleur contrôle sur les menaces liées aux programmes malveillants.

Forefront Client Security est en cours de développement. Microsoft prévoit de publier une version bêta du produit au cours du quatrième trimestre 2006.

Approche complète de la sécurité

Faisant partie des leaders de l'industrie informatique, Microsoft s'est engagé à fournir des produits plus sûrs et à aider ses clients à les déployer et à les gérer de manière efficace. Si Forefront est un composant clé de la stratégie de Microsoft pour la protection globale de la sécurité des clients professionnels, un grand nombre d'autres produits et d'initiatives jouent également un rôle important dans sa vision d'une infrastructure réseau sûre et correctement gérée.



Systèmes d'exploitation

Au cours de ces dernières années, Microsoft a consacré d'énormes ressources à la refonte de ses systèmes d'exploitation afin d'en faire les versions de Windows les plus sûres jamais conçues. Suite à la publication de Windows XP Service Pack 2 (SP2) et de Windows Server 2003 Service Pack 1 (SP1), un nombre significatif de failles importantes et critiques ont été éliminées, rendant ces deux systèmes d'exploitation plus résistants contre les programmes malveillants. Toutefois ces améliorations ne sont rien à côté de celles qui seront incluses dans les nouvelles versions de Windows Vista et Windows Server (nom de code « Longhorn »). Tout au long de la conception de Vista et Longhorn, l'objectif majeur a été la sécurité. Le résultat est un système d'exploitation renforcé sur lequel les utilisateurs peuvent exécuter les tâches les plus critiques et les plus confidentielles en toute sérénité.

Protection d'accès réseau (NAP)

Network Access Protection (NAP) est une plate-forme d'application de stratégies intégrée aux systèmes d'exploitation Windows Vista et Windows Server « Longhorn ». Elle permet une meilleure protection du réseau en définissant une stratégie de sécurité et en vérifiant l'état des ordinateurs

portables, ordinateurs de bureau et serveurs pour déterminer s'ils satisfont aux exigences de la stratégie. Les stratégies liées à l'état du système peuvent notamment inclure (sans toutefois s'y limiter) les niveaux de mises à jour logicielles, les signatures antivirus, les paramètres de configuration spécifiques, les ports ouverts et fermés et les paramètres de pare-feu.

Lorsqu'un ordinateur client tente d'accéder au réseau, NAP détermine si le client est en conformité avec les stratégies informatiques de l'organisation. Si tel est le cas, le client se voit octroyer les droits d'accès appropriés au réseau. Dans le cas contraire, un accès limité peut être accordé à l'ordinateur, mais généralement il est systématiquement mis en quarantaine, pendant qu'il est automatiquement mis à jour en vue de sa remise en conformité. Une fois l'ordinateur conforme, il est en mesure d'accéder au réseau.

Protection des informations

Si une approche de défense en profondeur de la sécurité doit considérer la protection des données au sein du réseau de l'entreprise, elle doit également inclure comment protéger les informations en dehors de ce périmètre sécurisé. Microsoft Windows Rights Management Services (RMS) optimise l'infrastructure de sécurité d'une entreprise à l'aide de stratégies d'utilisation persistantes qui demeurent avec les informations, tant en ligne que hors connexion, à l'intérieur et à l'extérieur du pare-feu.

Les applications compatibles avec RMS permettent aux entreprises de protéger leurs informations numériques sensibles, telles que rapports financiers, spécifications de produits, données clients ou messages électroniques confidentiels, contre une utilisation ou distribution non autorisée. Par exemple, une entreprise peut exiger que le destinataire d'un message électronique spécifique ne soit pas autorisé à faire suivre le message, l'imprimer, copier et coller son contenu ou utiliser la fonction d'impression d'écran pour effectuer une capture du contenu. De la même façon, des stratégies peuvent être implémentées pour empêcher certains utilisateurs d'accéder au contenu d'un document Word ou d'afficher des cellules spécifiques d'une feuille de calcul Excel. Ainsi, les données peuvent être contrôlées avec une grande précision, minimisant les risques de fuite d'informations pour les entreprises.

Services

Un grand nombre d'entreprises ont recours à des services gérés plutôt que de déployer et gérer elles-mêmes les solutions. Si cela est particulièrement vrai pour les entreprises dont le budget ou l'expertise interne est limité, ce scénario concerne également de très grandes entreprises à la recherche de nouvelles capacités.

Microsoft Exchange Hosted Services offre un ensemble de services de sécurité de messagerie entièrement gérés et hébergés qui protègent les entreprises contre les programmes malveillants transmis par la messagerie, sont en conformité avec les exigences en matière de rétention de données, chiffrent les données pour en préserver la confidentialité et maintiennent l'accès à la messagerie pendant et après des situations d'urgence. Ces services réduisent les investissements supplémentaires nécessaires, libèrent des ressources humaines informatiques qui pourront ainsi se concentrer sur d'autres initiatives importantes pour l'entreprise, et limitent les risques liés aux messages avant que ceux-ci n'atteignent le pare-feu de l'entreprise.

Gestion des identités

L'objectif de la sécurité réseau et du contrôle d'accès consiste à identifier *qui* veut accéder aux informations de l'entreprise et à *quelles* informations il tente d'accéder. Par conséquent, les processus, technologies et stratégies de gestion de l'accès et des identités jouent un rôle crucial dans toute solution de sécurité. Les produits de sécurité Microsoft sont liés entre eux à l'aide d'une puissante infrastructure de gestion des identités basée sur Active Directory et sur plusieurs autres produits associés. Ces produits permettent aux entreprises de gérer les identités numériques et de spécifier comment elles sont utilisées pour l'accès aux ressources. L'intégration de ces fonctionnalités dans les produits Forefront permet de mettre en œuvre des solutions à « authentification unique », capables d'englober plusieurs entreprises.

Gestion des systèmes

Microsoft propose une vaste gamme d'outils de gestion et de création de rapports permettant des opérations sophistiquées de collecte, d'analyse et de création de rapports d'événements, ainsi que des outils permettant de créer et d'appliquer les meilleures pratiques en matière de sécurité. Le principal outil de gestion de systèmes de Microsoft est Microsoft Operations Manager (MOM), une solution de gestion complète qui optimise de manière radicale la disponibilité, les performances et la sécurité des réseaux et des applications Windows. MOM permet la gestion centralisée et la résolution automatique de problèmes de dizaines de milliers d'ordinateurs, en surveillant de manière continue les opérations des utilisateurs, des applications logicielles, des serveurs et des ordinateurs de bureau.

L'une des tâches courantes de la gestion de la sécurité est la gestion appropriée des correctifs. Les applications Systems Management Server (SMS) et Windows Server Update Services (WSUS) permettent la distribution automatique de logiciels, mises à jour et correctifs pour les systèmes d'exploitation et applications Microsoft. En outre, SMS inclut des outils de gestion de correctifs améliorés pour les périphériques mobiles et les produits non Windows installés dans l'entreprise. Grâce à leur intégration avec Active Directory, les outils de gestion de distribution de logiciels et de correctifs de Microsoft peuvent être contrôlés à grande échelle avec précision, par le biais de mécanismes basés sur des stratégies.

Outils de développeurs

Un grand nombre d'entreprises développent et utilisent des applications personnalisées. Dans la mesure où les fonctionnalités de beaucoup de ces applications sont essentielles à l'entreprise, il est impératif que ces dernières soient aussi sécurisées que les produits fournis par Microsoft et d'autres fournisseurs. Dans le cas contraire, ces applications personnalisées peuvent présenter des failles de sécurité, particulièrement celles provenant de l'intérieur de l'entreprise.

Ces dernières années, Microsoft a fait de grandes avancées dans le domaine de la conception et du développement de logiciels sécurisés, ce qui a mené au processus de cycle de développement sécurisé (ou SDL, Security Development Lifecycle). Le processus SDL regroupe les meilleures pratiques applicables à chaque étape de la création de logiciels. Utilisé par l'ensemble des développeurs de Microsoft, il est désormais disponible au grand public⁴.

4

SDL est pris en charge par des outils de développement tels que Visual Studio 2005, ce qui permet à des développeurs individuels ou des équipes de développement de logiciels de créer des solutions Windows, Web, Office et mobiles dynamiques, tout en étant plus productifs. Visual Studio aide les développeurs à générer du code sécurisé, grâce à l'utilisation de code managé et de diverses autres techniques. Visual Studio contient également de nombreux outils permettant de créer des applications sécurisées, notamment l'outil TAMT (Threat Analysis and Modeling Tool). Cet outil permet à un développeur d'entrer des sources de données, utilisateurs, rôles, systèmes et d'autres informations afin de générer une analyse des menaces pour leur application. En outre, il créera divers cas d'utilisation et autres points de test permettant aux développeurs de réduire les risques générés par leur code.

Microsoft et une gestion optimale de la sécurité

Microsoft offre un portefeuille de produits de sécurité particulièrement complet, garantissant une sécurité de bout en bout pour les ordinateurs clients, l'accès aux réseaux, les serveurs ainsi que les données stockées sur ces derniers. Il n'en reste pas moins que cela ne constitue que l'élément initial d'une solution vraiment sécurisée. Si l'accès à une vaste gamme de technologies de sécurité constituait la réponse, les problèmes liés à la sécurité auraient diminué ces dernières années au lieu d'augmenter. En réalité, la plupart des défis auxquels les clients sont maintenant confrontés dans le domaine de la sécurité sont liés non pas aux technologies proprement dites mais plutôt au déploiement et à la gestion appropriés de ces dernières. Par exemple, le Gartner Group a trouvé que jusqu'à 65 % de l'ensemble des failles de sécurité étaient dues à une administration ou une configuration erronée. La sécurité est un domaine complexe et les relations entre de nombreux produits, conçus par des fournisseurs différents, peuvent parfois s'avérer délicates. Il n'est donc pas surprenant que même les réseaux les mieux gérés présentent des failles inattendues.

Conscients du fait que la partie opérationnelle de la sécurité est au moins aussi importante que les technologies - un pare-feu incorrectement configuré ne peut qu'engendrer des problèmes - les développeurs de Microsoft concentrent la majeure partie de leurs efforts sur les différents aspects opérationnels de la sécurité. Grâce à l'intégration et à une administration simplifiée, en d'autres termes à la « facilité de sécurisation » de l'infrastructure, Forefront permet aux entreprises de :

- centraliser l'administration de la sécurité ;
- parvenir à une meilleure intégration avec l'infrastructure existante ;
- éviter les erreurs de configuration ;
- déployer une sécurité omniprésente ;
- disposer d'une vue homogène de la sécurité du réseau.

La résolution de ces problèmes permet de sécuriser davantage le réseau : les configurations sont correctes, la sécurité est déployée aux emplacements adéquats, plutôt que là où son implémentation est la plus facile pour le développeur, et la console d'administration de la sécurité permet d'identifier précisément ce qui se passe sur l'ensemble du réseau.

L'exécution d'opérations unifiées de collecte de données, de création de rapports et d'analyse dans l'ensemble des produits permet aux administrateurs de s'assurer que la protection des données est conforme aux stratégies de l'entreprise en matière de sécurité et qu'elle respecte la stricte réglementation en vigueur. En outre, il n'est plus nécessaire d'engager des dépenses coûteuses pour former ou reformer le personnel administratif en vue de l'utilisation de diverses consoles de gestion ou de rapports indépendantes.

L'importance que Microsoft accorde aux aspects opérationnels de la sécurité et, en particulier, à la manière dont les technologies doivent s'intégrer aux stratégies de sécurité d'une entreprise et les incorporer, permet d'améliorer la sécurité de l'infrastructure informatique de l'entreprise. En outre, cette attitude permet de faire évoluer plus rapidement la sécurité, de manière à passer d'une technologie réactive, servant simplement à « éteindre l'incendie », à une infrastructure offrant davantage de souplesse pour l'entreprise et lui permettant d'atteindre des objets commerciaux stratégiques. Pour

décrire cette évolution, Microsoft a conçu un modèle d'optimisation d'infrastructure⁵. Il s'agit d'une structure permettant à une entreprise d'appréhender rapidement la valeur stratégique et les avantages commerciaux que représente pour elle la transition d'un niveau de maturité « de base » (où l'infrastructure informatique est généralement perçue comme un centre de coût) vers une utilisation plus « dynamique », où la valeur commerciale de l'infrastructure informatique est clairement identifiée et où cette dernière est considérée comme un atout commercial stratégique et un « facilitateur métier ». L'approche de Microsoft de la sécurité est conforme à ce modèle. Microsoft peut aider une entreprise, dont la sécurité consiste en un simple pare-feu, à évoluer vers une solution de sécurité complète, basée sur des stratégies, qui lui permettra de protéger de manière proactive ses informations et d'accorder l'accès approprié aux employeurs, partenaires et clients.

Grâce à une intégration à plusieurs niveaux dans l'infrastructure informatique existante et à une gestion centralisée simplifiée, les produits de sécurité Microsoft Forefront offrent une protection et un contrôle renforcés permettant aux administrateurs de sécuriser de manière optimale l'environnement de leurs entreprises.

⁵ <http://www.microsoft.com/windowsserversystem/solutions/io/default.aspx>

Ressources connexes

Pour obtenir les informations les plus récentes à propos des produits de sécurité Microsoft Forefront destinés aux entreprises, consultez :

Microsoft Forefront : <http://www.microsoft.com/france/forefront/default.aspx>

Internet Security and Acceleration (ISA) Server 2006 : <http://www.microsoft.com/france/isaserver/default.aspx>

Intelligent Application Gateway (IAG) : <http://www.microsoft.com/isaserver/whale/default.aspx>

Forefront Server Security : <http://www.microsoft.com/france/antigen/default.aspx>

Forefront Client Security : <http://www.microsoft.com/france/forefront/clientsecurity/default.aspx>

Pour en savoir plus sur les autres produits de Microsoft dédiés à la sécurité, consultez :

Systemes d'exploitation

Windows Vista : <http://www.microsoft.com/france/technet/produits/windowsvista/default.aspx>

Windows XP : <http://www.microsoft.com/france/technet/prodtechnol/winxpro/default.aspx>

Windows Server 2003 : <http://www.microsoft.com/france/windows/windowsserver2003/default.aspx>

Windows Server « Longhorn » : <http://www.microsoft.com/france/windowsserversystem/longhorn/default.aspx>

Protection d'accès réseau (NAP)

Protection d'accès réseau (NAP) : <http://www.microsoft.com/technet/itsolutions/network/nap/default.aspx>

Services

Microsoft Exchange Hosted Services : <http://www.microsoft.com/exchange/services/default.aspx>

Protection des informations

Windows Rights Management Services : <http://www.microsoft.com/france/technet/produits/win2003/RMS.aspx>

BitLocker : <http://www.microsoft.com/france/technet/produits/windowsvista/security/bitlockr.aspx>

Système de fichiers EFS (Encrypting File System) : <http://www.microsoft.com/technet/security/topics/cryptographyetc/efs.aspx>

Gestion des identités

Active Directory : http://www.microsoft.com/france/technet/produits/win2003/AD_ADAM.aspx

Certificate Lifecycle Manager (CLM) : <http://www.microsoft.com/windowsserversystem/clm/default.aspx>

MIIS : <http://www.microsoft.com/france/miis/default.Asp>

ADFS (Active Directory Federation Services) :

http://www.microsoft.com/WindowsServer2003/R2/Identity_Management/ADFSwhitepaper.aspx

Gestion des systèmes

Microsoft Operations Manager (MOM) : <http://www.microsoft.com/france/mom/default.aspx>

SQL Server 2005 : <http://www.microsoft.com/france/sql/sql2005/default.aspx>

SMS (Systems Management Server) : <http://www.microsoft.com/france/sysmans/default.aspx>

WSUS (Windows Server Update Services) : <http://www.microsoft.com/france/technet/produits/win2003/WSUS.aspx>

Outils pour développeurs et conseils

SDL (Security Development Lifecycle) : <http://www.microsoft.com/france/msdn/securite/sdl.aspx>

Visual Studio 2005 : <http://www.microsoft.com/france/msdn/vstudio/default.aspx>