Microsoft Forefront Client Security bousculera-t-il le marché ?

L'intégré plutôt que les modules indépendants

Berverly Hills (USA) – Microsoft Forefront Client se veut une solution complète et homogène de protection des ordinateurs de bureau, des ordinateurs portables et des systèmes d'exploitation serveur des entreprises contre les programmes malveillants. Protection complète, car *« avec ses fonctions de sécurité réactives, Forefront Client Security permet la détection et la suppression à la demande, selon un planning ou en temps réel, de virus, logiciels espions, spams, rootkits et autres menaces émergentes, »*affirme Margaret Dawson, Responsable des produits de sécurité et d'accès chez Microsoft. Quant aux demandes spécifiques de produits uniquement antivirus ou spam par les entreprises ? *« Nous n'avons enregistré aucune demande en ce sens. Les entreprises souhaitent surtout bénéficier d'une sécurité globale reposant sur une plate-forme cohérente et performante, »* rétorque Margaret Dawson.

Forefront Client Security est disponible sous forme de licence à partir d'environ 13 dollars par utilisateur ou équipement pour un an d'utilisation, auxquels il faut ajouter environ 2.500 dollars pour la console d'administration.

Ce client est né d'un développement Microsoft reposant sur son apprentissage des technologies rachetées depuis quatre ans, et en partie utilisées pour créer Windows Live OneCare. En effet, on retrouve dans le portefeuille de l'éditeur : Gecad (antivirus racheté en juin 2003), Giant Company (antispyware racheté en décembre 2004), ou encore Sybari et Frontbridge (antivirus et antispam d'entreprise rachetés en 2005). *« Nous sommes convaincus qu'une solution de sécurité doit être complète, intégrée et simplifiée. En ce domaine, l'intégré l'emporte sur le best-of-breed. Toutefois, Microsoft propose une approche spécifique favorisant l'intégration optimale. En effet, nous ne nous contentons pas de racheter des produits et de les ajouter au catalogue, mais nous les intégrons au maximum dans notre architecture afin de favoriser les synergies et l'efficacité d'une politique globale de sécurité, »*souligne Margaret Dawson.

Une administration centralisée

Mais surtout, si la solution déployée peut fonctionner en produit indépendant, elle bénéficie surtout d'une console d'administration centralisée promettant d'assurer la cohérence du système d'information de l'entreprise de bout en bout.*« Parce que gérer c'est aussi voir et comprendre ce qui se passe, Forefront Client Security peut générer des rapports de sécurité détaillés et un tableur de bord de sécurité, »*affirme Margaret Dawson. En effet, l'intégration concerne autant Forefront que System Center, plateforme d'administration stratégique pour l'éditeur de Redmond. En effet, Microsoft mise sur l'intégration étroite entre les solutions de sécurité et d'administration système. Pourtant, *« la console d'administration reste dédiée à Forefront de façon indépendante, mais sera bientôt intégrée à System Center, »* reconnaît Margaret Dawson. Bien entendu, l'éditeur souligne que l'intégration applicative est facilitée via les annuaires Active Directory ou ISA Server (voir ci-dessous).

Des laboratoires répartis sur la planète

Enfin, comme annoncé l'an dernier, Microsoft a initié l'ouverture de laboratoires de surveillance

virale et de sécurité mondiaux, indispensable à tout éditeur de logiciels de sécurité. Outre son laboratoire de Redmond, l'éditeur a renforcé son dispositif avec deux premières ouvertures en Irlande et au Japon.*« Bien entendu, nous poursuivons ce déploiement international. Par ailleurs, nous échangeons des informations en continu avec les autres éditeurs spécialisés, une collaboration indispensable pour lutter efficacement et coordonner les efforts, »*rappelle Margaret Dawson. Il est vrai que les moteurs Forefront sur les serveurs combinent l'utilisation de divers moteurs antivirus, pour lesquels Microsoft a signé des accords.

Une panoplie serveur déjà bien fournie

Début 2005, Microsoft avait racheté Sybari Software, éditeur américain de solutions de sécurité. Ses solutions Antigen font fonctionner simultanément plusieurs moteurs antivirus (Computer Associates, Kaspersky, Sophos, etc.) sur les serveurs. Afin de protéger ses serveurs de messagerie et de collaboration contre les virus, les vers, les courriers indésirables et autres contenus inappropriés, Microsoft a utilisé ces technologies pour concevoir trois solutions Microsoft Forefront Security : pour Exchange Server, pour SharePoint et pour Office Communications Server. L'analyse successive de plusieurs moteurs antiviraux permet d'atteindre une protection efficace. Et Forefront peut empiler jusqu'à neuf moteurs (parmi ceux de Microsoft, CA InoculateIT, CA Vet, Norman, Sophos, Authentium, Kaspersky, VirusBuster et AhnLab). *« Pour des résultats efficaces et performants, nous recommandons un maximum de cinq moteurs sur les serveurs, »* précise néanmoins Margaret Dawson.

Toujours côté serveur, L'éditeur propose Internet Security and Acceleration Server 2007 et Whale Communications Intelligent Application Gateway. ISA Server inspecte le contenu des paquets et leur conformité aux attentes des applications, et peut aussi les déchiffrer et les chiffrer à nouveau si nécessaire. Grâce à un rachat de Whale Communications en mai 2006, Microsoft peut proposer Intelligent Application Gateway pour protéger les applications Web et VPN SSL (stratégies de sécurité, inspection de contenu avec règles, etc.).

Qui survivra ?

Une solution administrée en central sur les postes, une force de frappe sur les serveurs? Microsoft est armé pour se positionner fortement sur les systèmes d'information. Pourra-t-il convaincre les entreprises que ses rachats de spécialistes reconnus lui ont permis de créer une gamme intégrée, cohérente et efficace ? L'année 2007 sera certainement un tournant décisif. Et si Microsoft s'impose, le marché devrait s'orienter vers des plates-formes intégrées de sécurité, avec accélération des concentrations et rachats multiples. Et bien évidemment son lot de victimes?