# Sophos poursuit sur la voie de l'intégration

L'éditeur lance une nouvelle solution qui va mettre au défi ses principaux concurrents.

Présentée dans ses locaux d'Oxford, cette nouvelle solution « all in one » cible les professionnels. Sa particularité, une intégration forte, puisque qu'elle combine, antivirus, antispyware, anti-rootkit, pare-feu, prévention d'intrusion et contrôle des applications?

Baptisée 'Endpoint Security and Control 7.0', cette nouvelle application vise à renforcer la productivité des utilisateurs et à réduire les coûts récurrents d'administration des réseaux. Dans ce but, elle permet aux administrateurs d'accéder à des informations détaillées sur la conformité des systèmes.

*« Pour tenir compte des changements constants à la fois dans l'environnement des affaires et dans la nature des menaces, la sécurité doit être associée à l'ensemble des processus commerciaux et informatiques »*, déclare John Pescatore, VP Distinguished Analyst chez Gartner; Inc. *« Les solutions de sécurité que les entreprises installent sur leurs réseaux, leurs serveurs et leurs PC doivent constituer des plates-formes capables d'être chaque année plus efficaces tant dans le traitement rapide des menaces nouvelles que dans la protection contre les plus anciennes. »*

Les entreprises peuvent déployer à travers leur réseau un client unique, capable de détecter en une seule passe les virus, les spywares et les adwares, mais également les fichiers ou comportements suspects et les applications non autorisées comme celles de voix sur IP (VoIP), de messagerie instantanée ou de jeu.

Selon le communiqué de Sophos cela permet : *« d'éviter la multiplication des solutions individuelles qui effectuent chacune leur propre analyse. Les entreprises peuvent également appliquer leurs politiques de sécurité et de contrôle à des dizaines de milliers d'ordinateurs Windows, Mac et Linux à partir d'une seule console. En synchronisant la solution avec Microsoft Active Di rectory, ces politiques de sécurité seront automatiquement appliquées à tout nouvel ordinateur s'ajoutant au réseau. »*

En ce qui concerne la protection contre les menaces 'Zero Day', qui ont une fâcheuse tendance à se généraliser, les ingénieurs des 'labs' ont mis au point un module permettant la prévention proactive contre les intrusions.

Celui-ci dispose d'une technologie dite 'Behavioral Genotype', reposant sur la surveillance des comportements suspects. Par exemple, une détection avant exécution des fichiers suspects, des dépassements de mémoire tampon (buffer overflow), une analyse des temps d'exécution, l'évolution des processus.

D'après Christian Pijoulat, dg de Sophos France et Europe du Sud : *« Son système d'analyse unique est le moyen le plus rapide et efficace de détecter les menaces pesant sur la sécurité comme sur la productivité. Alors que les autres éditeurs obligent leurs clients à s'appuyer sur des solutions séparées, notre solution réellement intégrée permet aux entreprises d'assurer à la fois la sécurisation et le contrôle de leurs réseaux informatiques. »*

Signalons enfin, que la nouvelle version de la console d'administration est à même d'effectuer les

déploiements, les mises à jour, la publication de rapport, et l'application des politiques de sécurité à partir d'un point unique. L'interface est composée d'un tableau de bord pour surveiller en un coup d'oeil les risques de dissémination à l'échelle du réseau. Il donne également aux entreprises la possibilité de bloquer ou d'autoriser l'usage d'applications potentiellement indésirables, qui peuvent avoir un impact sur la sécurité mais aussi sur le plan juridique, de la maintenance ou de la productivité.