Vision 2007 : Symantec affine sa stratégie pro

Las Vegas. Profitant de la dixième édition du salon Vision, le groupe vient de présenter **Endpoint Protection 11.0 et Symantec Network Access Control 11.0.** Le nom de code du projet est Hamlet, à priori, il n'y a rien de revanchard là-dedans contrairement à la plus fameuse des pièces du théâtre shakespearien.

L'éditeur américain bien connu pour son logiciel destiné à la protection des particuliers : Norton, vient de franchir un nouveau cap, cette fois dans la protection des sociétés.

Afin de protéger les entreprises contre les nouvelles et anciennes menaces, Endpoint Protection intègre des technologies proactives d'analyse de comportement d'application et de communication réseau, et combine des solutions de sécurité multiples telles que l'antivirus, l'anti-logiciels-espions, le pare-feu, l'IPS ou prévention d'intrusion agent et réseau.

Cette nouvelle application fait tout cela dans un seul agent, et elle peut être supervisée depuis une interface unique.

Dans les faits, elle combine les solutions de Symantec, Sygate, Whole Security et Veritas. Cette nouvelle offre profite du soutien du réseau Global Intelligence de Symantec et de ses huit centres « Security Response » et des quatre centres « Security Opération. »

D'après Tom Kendra, en charge de la division sécurité et management des données chez Symantec, *« cette nouvelle application pour l'instant en version Beta mais dont la mouture finale sera disponible en septembre, va relever le niveau de protection en entreprise et en simplifier l'administration. »*Kendra précise que *« Endpoint offre un gain de productivité et une réduction des coûts »* malheureusement l'éditeur ne donne pas de chiffres sur le retour sur investissement.

La console de management qui centralise tout est la version 11.0 de Network Access Control (NAC).

Symantec met à disposition de ses clients ses équipes pour faciliter l'implémentation au cas par cas. NAC est un module optionnel intégré à Endpoint qui permet de partir à la découverte de l'état de santé du réseau et d'en faire une évaluation. Cette interface permet également la mise en place de politiques de sécurité.

Les points clés de cette offre

Symantec fait la part belle à de nouvelles technologies qui sont le fruit de plusieurs années d'acquisition dans le domaine de la sécurité.

D'abord, le logiciel intègre la technologie dite de « deep scanning » de Veritas. Cette dernière permet entre autres de remédier au problème des Rootkits qui échappent le plus souvent à la détection.

Une nouvelle approche de protection proactive permet de lutter contre les menaces inconnues ou zero-day.

Concrètement, l'application lance des scans reposant sur le comportement de la machine et de son utilisateur, notamment en surveillant les processus en cours d'exécution. En analysant ces « bons et mauvais comportements » le taux de faux positifs est réduit.

Notons aussi que Symantec a intégré la technologie développée par Whole Security : Proactive Threat Scan. Cette dernière détecte et bloque les malwares qui n'ont pas encore de signatures afin d'empêcher qu'elles ne s'exécutent. Le contrôle des équipements permet également aux sociétés de réduire voir interdire l'utilisation des clés USB ou des disques de back-up afin de limiter le risque lié à la perte de données sensibles.

Endpoint dispose aussi d'une nouvelle technologie de prévention des intrusions baptisée GEB pour Generis Exploit Blocking. En positionnant cette IPS directement au point d'entrée du réseau de l'entreprise, cela permet d'éviter la propagation du code malveillant.

Selon l'éditeur, GEB *« bloque tous les nouveaux exploits d'une vulnérabilité y compris les variantes. »* Notons que le pare-feu est là aussi signé Sygate, point intéressant, il est aussi capable de s'ajuster de façon dy namique et d'inspecter les contenus cryptés.

Une version bêta de Endpoint Protection est disponible sur ce lien