Pour en finir avec le mythe de la solution miracle en matière de lutte antimalware

Les produits de sécurité, une spirale sans fin

En matière de protection des terminaux, on a facilement le sentiment d'avoir constamment une longueur de retard — et c'est effectivement bien trop souvent le cas. Dès qu'une nouvelle stratégie d'attaque par logiciel malveillant (malware) voit le jour, vous déployez un nouveau produit spécifique pour la contrer. Six mois plus tard, une nouvelle menace fait surface, et un nouveau produit est nécessaire pour la combattre. Les mois défilent, et le même scénario se répète. C'est une course incessante.

Consolidation et coordination de la sécurité des terminaux

En réalité, ce n'est pas d'une technologie unique, l'« arme absolue », dont vous avez besoin pour protéger vos terminaux. Mais de plusieurs technologies, non pas juxtaposées mais unies, qui fonctionnent de concert, de manière intégrée et automatisée. Avec un tel système, même si une menace parvient à contourner une technologie située à un niveau de défense donné, cette dernière tire des enseignements de cette détection et les diffuse aux autres technologies, qui seront dès lors mieux à même de bloquer la menace avant qu'elle n'entre en action.

La nouvelle génération de technologies antimalware et de protection des terminaux de McAfee offre une structure de défense véritablement intégrée et coordonnée, spécialement conçue pour ces systèmes, où les différents éléments collaborent entre eux pour transformer les nouvelles informations acquises en actions en temps réel. Cette structure propose notamment les fonctions suivantes :

- **Apprentissage automatique alimentant l'analyse statique et l'analyse comportementale** : Les techniques avancées d'apprentissage automatique fournies par McAfee® Real Protect sont utilisées pour comparer d'un point de vue statistique les fichiers suspects aux menaces connues, sans recourir aux signatures.
- **Confinement des applications suspectes** : Le confinement d'application dynamique proposé par McAfee protège les terminaux contre les logiciels malveillants de type « jour zéro » encore inconnus, en empêchant les processus d'exécuter des actions généralement associées au malware.
- **Analyse en environnement sandbox** : Les logiciels malveillants ciblés les plus avancés sont démasqués par le déclenchement de l'exécution des fichiers suspects dans un environnement sécurisé, McAfee Advanced Threat Defense, et une analyse ultraprécise de leur base de code complète.

intel Security

Chacune de ces technologies offre des fonctionnalités antimalware essentielles. Ensemble, elles forment un système de défense multiniveau qui arrête net la grande majorité des menaces avant même qu'elles n'infectent le « patient zéro », puis assure une réponse coordonnée en temps quasi réel, sans intervention manuelle.

Briser la spirale des produits de sécurité

Les logiciels malveillants continuent d'évoluer, et il n'existe aucune solution miracle capable de vous protéger contre l'intégralité de ces menaces. Jongler avec plusieurs solutions isolées exige plus de temps et de ressources et accroît la complexité pour des équipes de sécurité déjà mises à rude épreuve. L'heure est venue d'adopter une approche plus intelligente.

En savoir plus

Pour en savoir plus sur la façon dont Real Protect, le confinement d'application dynamique et Advanced Threat Defense de McAfee collaborent, téléchargez le livre blanc **Pour en finir avec le mythe de la solution miracle en matière de lutte antimalware**.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/fr