

Microsoft Security Essentials antivirus gratuit et complet ?

26/08/2010 09:11 par Jean-Christophe B.

Une fois votre licence de Windows acquittée, rien ne vous oblige à investir dans une solution de sécurité payante. En effet, en complément de son pare-feu bidirectionnel qui constitue un premier rempart contre les intrusions, vous pouvez télécharger gratuitement l'antivirus Microsoft Security Essentials. Celui-ci disponible depuis septembre 2009 vous procurera une protection en temps réel contre les virus, les logiciels espions, logiciels malveillants et autres menaces néfastes.

INTRODUCTION

Compléter la sécurité de Windows XP, Vista ou 7 avec l'antivirus MSE



Microsoft Security Essentials est le logiciel antivirus gratuit proposé par Microsoft à tous les possesseurs d'une licence Windows XP, Vista et Seven, avec des versions distinctes en 32 et 64 bits pour les deux derniers OS. En plus du pare-feu logiciel intégré, ce successeur de Windows Live OneCare vient renforcer la sécurité globale du système en délivrant une protection contre les virus, les logiciels espions, les rootkits, chevaux de Troie et toutes autres nouveaux virus non identifiés.

Un antivirus comme les autres ou davantage ?

C'est un antivirus qui reprend la

majeure partie des fonctionnalités de ses concurrents, gratuits et payants. Qu'entendons-nous par -là ? La protection en temps réel, une base de définition de virus et de logiciels espions, des mises à jour automatiques, différents types d'analyses (rapide, complète, personnalisée), une mise en quarantaine des menaces et un comportement à adopter en l'occurrence, un scan automatique planifié et bien d'autres paramètres utiles que nous passerons en revue.



Sitôt installé, Windows Defender se désactive au profit de MSE plus complet...



L'installation de Microsoft Security Essentials débute, après que le programme Windows Genuine Advantage (WGA) a bien déterminé que votre copie Windows est originale. Si Windows Defender est actif sur votre machine celui-ci sera désactivé. En effet, Microsoft Defender devient obsolète étant donné que Microsoft Security Essentials inclus le même anti-spyware en commun et bien plus de services. Beaucoup d'utilisateurs se plaignent du fait que les mises à jour ne sont pas toujours fonctionnelles (codes d'erreurs 0x8*****...). En plus de vous présenter ce produit et ses caractéristiques, nous vous indiquerons comment procéder manuellement à l'actualisation des définitions de virus.

MICROSOFT SECURITY ESSENTIALS : LES FONCTIONNALITÉS ESSENTIELLES

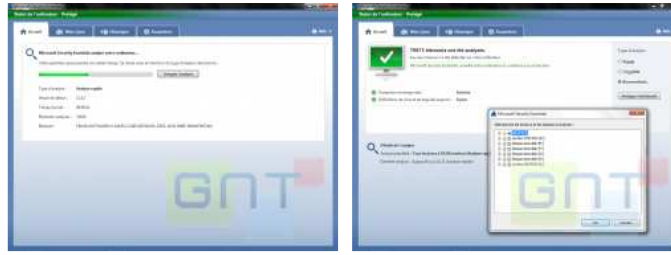
Trois statuts indiquent l'état en cours de la machine

Microsoft Security Essentials comme nous l'avons précisé en introduction est une application qui protège Windows en temps réel contre les virus, les logiciels espions et les autres logiciels potentiellement dangereux. Pour vous faire une opinion de l'efficacité de MSE nous vous renvoyons au [dernier rapport d'août 2010 du Virus Bulletin](#) mais sachez que les tests ont été passés avec brio. Une fois l'outil installé, une première analyse s'effectue. A l'issue de ce scan le statut de l'ordinateur s'affiche sous forme d'icone dans la zone de notification. Pour le plus grand bonheur de tous, la simplicité est de mise, une maison verte indique que votre ordinateur est "protégé", une jaune qu'il y a un danger et que le PC est "potentiellement non protégé". Enfin, une maison rouge affiche sans ambiguïté une machine "en danger". Ces statuts sont repris dans l'onglet accueil :



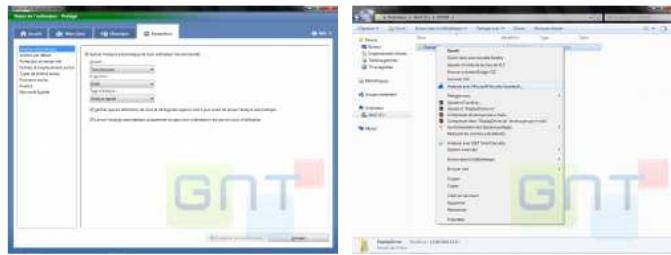
Trois analyses à la demande

Un double clic sur l'icône de MSE ouvre le panneau d'accueil. Ce dernier affiche l'état de la machine en résumant l'essentiel, à savoir, si la protection en temps réel est en route et si les définitions de virus et de logiciels espions sont à jour. C'est ici que l'utilisateur procède à la demande aux trois types d'analyses disponibles. L'analyse rapide se consacre aux zones de l'ordinateur les plus susceptibles d'être infectées par des logiciels malveillants, la complète s'intéresse à toutes les zones de l'ordinateur et est donc de fait plus longue. L'analyse personnalisée permet comme son nom l'indique de scanner uniquement des zones précises de l'ordinateur. Vous sélectionnez dans ce cas les lecteurs et dossiers que vous jugez suspects.



Analyse contextuelle et analyse planifiée

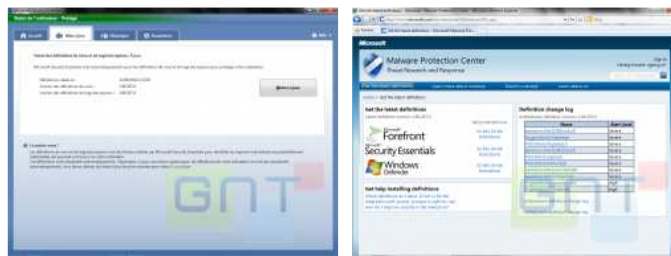
Il suffit de cliquer avec le bouton droit sur l'élément (dossier ou fichier) dont vous vous méfiez et de valider "Analyser avec Microsoft Security Essentials..." pour avoir en quelques secondes un rapport, c'est l'analyse contextuelle. Pour activer une analyse planifiée, c'est-à-dire qui se déclenche sans votre intervention à intervalle régulier, en bas de l'onglet Accueil cliquez sur Modifier les paramètres. Vous vous retrouvez dans la rubrique "Analyse automatique". Cochez simplement la case "Activer l'analyse automatique de mon ordinateur (recommandé)" et répondez à trois questions, quand (le jour de la semaine), à environ (l'heure) et type d'analyse (rapide ou complète). Pour information, sachez que nous n'avons constaté aucun ralentissements de la machine dans le cadre de nos analyses sous Windows 7 (Intel Core2Quad, 4 Go de RAM) ni même sur notre netbook (Intel Atom N280 1,66 GHz, 1 Go de RAM).



MICROSOFT SECURITY ESSENTIALS : MISE À JOUR ET HISTORIQUE

Mise à jour automatisée Faut-il attendre Windows Update ?

En théorie, les mises à jour de Microsoft Security Essentials pour les définitions de virus et de logiciels espions sont automatiques, elles s'effectuent par l'intermédiaire de Windows Update tous les... Pour une actualisation plus régulière, il faut procéder soi-même et mettre la main à la patte. Rendez-vous dans l'onglet Mise à jour et pressez le bouton "Mettre à jour". Dans les secondes qui suivent, les nouvelles définitions s'installent. Vous pouvez alternativement récupérer la dernière mise à jour en 32 ou 64 bits, sous forme de fichier auto-exécutable sur le site [Microsoft Malware Protection Center](#) (MMPC).



Quand la mise à jour ne fonctionne pas...

Beaucoup d'utilisateurs se plaignent de l'échec des mises à jour des définitions et des mises à niveau de MSE, il n'y a qu'à se rendre sur le [site communautaire](#) en rapport pour s'en rendre compte. Ils rencontrent souvent des erreurs du type "0x8*****". La cause la plus fréquente est la désactivation du service Microsoft Update. Pour le relancer sous Vista/7, il suffit de cliquer sur Démarrer, et dans la zone de Recherches de taper "services.msc" (puis Entrée). Repérez le service "Windows Update", affichez à l'aide du bouton droit les Propriétés puis validez "Démarrer". D'autres causes sont encore possibles, il suffit de se référer au site Web d'assistance de Microsoft Security Essentials et de consulter les rubriques d'aide ou de saisir directement votre code erreur dans [Microsoft Answers](#).



L'historique QG des éléments dangereux...

C'est dans l'onglet Historique que l'on retrouve la liste des menaces détectées. Elles s'affichent en rouge jusqu'à ce que l'utilisateur décide d'une action et en vert lorsque l'élément a été supprimé. Vous pouvez bien entendu décider de maintenir l'objet suspect en quarantaine (menace désactivée mais pas supprimée) et ajourner votre décision ou autoriser l'élément si vous estimez qu'il s'agit d'un faux positif. Nous verrons, dans la partie consacrée aux paramètres que des scripts d'actions par défaut sont possibles en cas de découvertes de menaces.

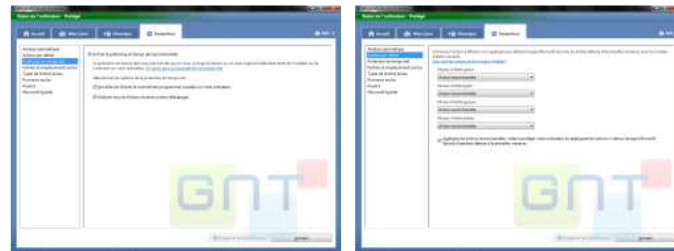


MICROSOFT SECURITY ESSENTIALS : LES PARAMÈTRES À LA LOUPE

Protection en temps réel, Actions par défaut

L'ultime onglet, Paramètres reprend la philosophie globale de MSE, tout y est clairement expliqué, et l'absence de technicité inutile ravira l'utilisateur lambda. La protection en temps réel est l'un des maillons forts de la solution antivirus/antispyware. Vous devez toujours veiller à ce qu'elle soit activée et que certains malicieux ne l'ont pas stoppée. Le rôle de cette détection proactive est essentiel. Elle s'intéresse aux nouvelles menaces via leur comportement, à la surveillance des programmes installés sur votre PC ainsi qu'à l'analyse des fichiers et pièces jointes téléchargés par le biais de votre client de messagerie électronique, logiciel de messagerie instantanée, etc.

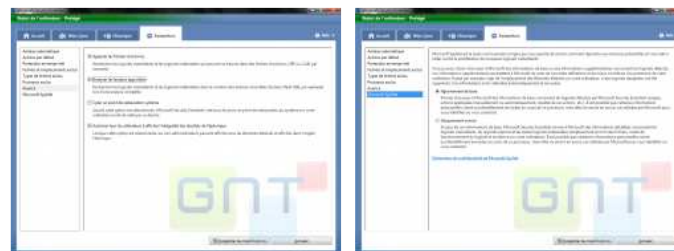
C'est dans la rubrique des actions par défaut que vous déterminerez l'action à réaliser en cas de découverte de menaces (action recommandée, supprimer, mettre en quarantaine, autoriser) et cela avec une action variable selon les différents niveaux d'alertes (grave, haut, moyen, faible). Nous conseillons aux néophytes de tout laisser positionner sur "Action recommandée", ainsi MSE agira au mieux.



Paramètres d'analyse avancée, MS Spynet

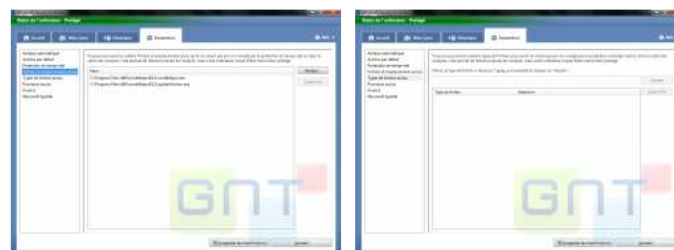
Il serait regrettable de ne pas se rendre dans les Paramètres et sous Avancé. C'est à cet endroit que vous pourrez affiner les réglages de MSE qui combinent comme les BitDefender, Eset et les autres des fonctionnalités bien utiles. Par défaut, l'analyse des fichiers archives (ZIP, CAB...) est activée. C'est désormais un incontournable et bien des logiciels malveillants sont inclus dans des fichiers compressés. Nous vous conseillons de mettre en route l'analyse des lecteurs amovibles. Celle-ci recherche des éventuelles menaces dans les clés USB que vous insérez occasionnellement, les cartes mémoires, les disques durs externes. La création d'un point de restauration système quotidien n'est pas cochée, et pour nous elle restera ainsi. Elle est à double tranchant car elle peut certes vous permettre de revenir à un point de restauration sain comme vous ramenez à un état de contamination si vous y faites appel, selon nous.

La rubrique Microsoft Spynet envoie en fonction de ce que vous avez coché à MS des informations de base ou détaillées à propos des logiciels malveillants et peut-être même des informations personnelles : "elles ne seront en aucun cas utilisées par Microsoft pour vous identifier ou vous contacter". Il manque selon nous une troisième option comme dans Windows Defender qui s'intitulerait, "je ne souhaite pas soumettre d'informations Microsoft Spynet". Nous vous invitons avant installation de MSE de prendre connaissance de la "Déclaration de confidentialité de Microsoft Security Essentials".



Exclusion d'emplacements, de fichiers, d'extensions et de processus

Il n'est pas rare que les programmes antivirus détectent des applications fiables comme étant des menaces potentielles. Pour éviter que certains de vos programmes de confiance soient systématiquement supprimés ou mis en quarantaine nous vous invitons à les ajouter en passant par la rubrique Fichiers et emplacements exclus, c'est ce que nous avons fait pour notre Scrabble en ligne et son fichier de mise à jour qui était détecté comme une menace. Il est également possible d'exclure des processus (processus exclus) des types de fichiers (*.jpeg, *.avi, *.mp3 ou autres) mais prenez garde avec cette fonctionnalité car une menace peut revêtir une extension différente et ne se trouve pas nécessairement dans un fichier *.exe, *.cmd, *.bat, *.pif, *.scr...



CONCLUSION

Un antivirus tout aussi correct que ses concurrents gratuits

Microsoft Security Essentials s'avère être à l'usage un antivirus/anti logiciel espion à la hauteur de ses concurrents gratuits. Il réunit les fonctionnalités attendues à savoir une base de définition de virus



régulièrement mise à jour via Windows update ou manuellement et une détection proactive pour lutter contre les nouvelles menaces. L'application surveille tous les fichiers joints que vous recevez par l'intermédiaire de votre navigateur Web, client e-mail, client de messagerie instantanée et analyse tous les éléments présents sur les lecteurs amovibles (une fois l'option cochée).

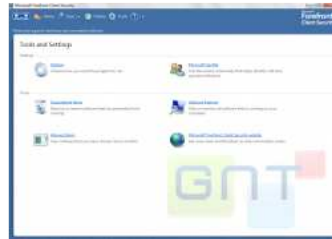
Un choix commode pour compléter sa défense

Beaucoup de particuliers se contentent du pare-feu intégré dans Windows et de l'antispysware Windows Defender. Pour rester dans l'esprit du gratuit, nous leur conseillons Microsoft Security Essentials en 32 ou 64 bits, selon la licence Windows qu'ils possèdent. Cette solution de sécurité reprend la fonctionnalité de lutte et de suppression des logiciels espions de Windows Defender (moteur et définitions communes), la protection en temps réel et lui ajoute les défenses classiques d'un véritable antivirus. De plus, les mises à jour sont assurées en transparence par Windows Update.



Microsoft ForeFront Client et Serveur

Pour les postes de travail en entreprise, il existe également une gamme de produits dédiée à la sécurité clients/serveurs que l'on retrouve sous le nom de Microsoft ForeFront 2010. Forefront reprend les fonctions similaire à MSE avec en plus des protections pour les serveurs d'applications (Exchange/Exchange Server, SharePoint), la périphérie du réseau (Microsoft Threat Management Gateway 2010, Microsoft Unified Access Gateway 2010).



LES PLUS

Antivirus et Anstispyware efficace et accessible à tous
Protection en temps réel et base de définition antivirus
Analyse rapide, complète, personnalisée, contextuelle
Scan des lecteurs amovibles, fichiers joints, fichiers téléchargés...

LES MOINS

Problème de MAJ récurrent rencontré par certains utilisateurs