



Fiche Technique

Outpost Security Suite Pro 2009

Une protection proactive pour des utilisateurs d'Internet intelligents

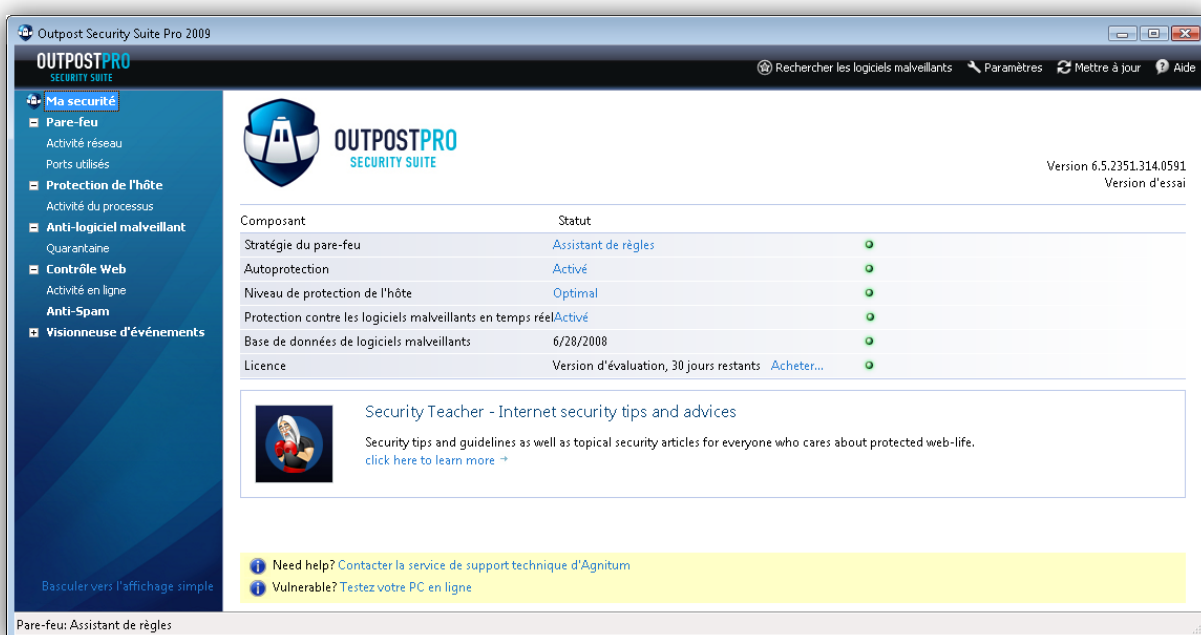
Pourquoi une protection proactive?

L'Internet d'aujourd'hui nécessite une toute nouvelle approche de la sécurité. Pratiquement tout est interconnecté et se passe en temps réel. Les menaces en font partie. Un logiciel de sécurité efficace doit être sur le qui-vive à chaque instant en cas de nouveaux logiciels malveillants encore plus pervers.

De nouveaux types de menace nécessitent de nouveaux types de protection. Les virus de distribution de masse et les vers donnent naissance à des attaques à but lucratif conçues pour dérober les identités, de l'argent et autres ressources électroniques de valeur par l'intermédiaire du hameçonnage et du « social engineering » (subversion psychologique).

Pour protéger entièrement un système contre ces nouveaux risques, une solution de sécurité efficace doit déployer une approche multicouche, fournir un blocage proactif basé sur le comportement de même qu'une détection plus traditionnelle de signatures reposant sur une base de données. Il doit également être facile à utiliser car, s'il ne l'est pas, il ne sera pas utilisé.

En se basant sur la protection bien connue d'Outpost Firewall Pro, Outpost Security Suite Pro d'Agnitum associe le meilleur des deux approches dans un seul produit intégré qui offre une protection personnalisable et une totale fiabilité. Outpost Security Suite Pro est sur ses gardes, protégeant les données 24 heures/24, 7 jours sur 7, quelles que soient les activités réalisées sur l'ordinateur.



The screenshot shows the Outpost Security Suite Pro 2009 interface. The window title is "Outpost Security Suite Pro 2009". The interface includes a sidebar with navigation options: "Ma sécurité", "Pare-feu", "Protection de l'hôte", "Anti-logiciel malveillant", "Contrôle Web", "Anti-Spam", and "Visionneuse d'événements". The main area displays the "OUTPOSTPRO SECURITY SUITE" logo and a table of components and their status.

Composant	Statut
Stratégie du pare-feu	Assistant de règles
Autoprotection	Activé
Niveau de protection de l'hôte	Optimal
Protection contre les logiciels malveillants en temps réel	Activé
Base de données de logiciels malveillants	6/28/2008
Licence	Version d'évaluation, 30 jours restants Acheter...

Below the table, there is a "Security Teacher" section with a small icon and text: "Security tips and guidelines as well as topical security articles for everyone who cares about protected web-life. click here to learn more". At the bottom, there are two yellow banners: "Need help? Contacter le service de support technique d'Agnitum" and "Vulnerable? Testez votre PC en ligne". The status bar at the bottom left reads "Pare-feu: Assistant de règles".

Technologies clés

- **Pare-feu bidirectionnel** pour protéger l'accès au réseau
- **Système de détection des intrusions (Intrusion Detection System - IDS) et protection Ethernet** pour une défense automatisée contre les sondes de failles de sécurité et les brèches de sécurité internes
- **Scanner antivirus et anti logiciel espion associés** pour une défense tout-en-un contre les logiciels malveillants
- **Protection de l'hôte** pour bloquer de façon proactive les menaces inconnues
- **Anti-spam** pour libérer votre boîte de réception des pourriels
- **Sécurité Web & transactions** vous protège des risques d'Internet
- **Autoprotection** pour assurer la continuité de la protection
- **Configurations automatisées pouvant être mises à jour** pour simplifier la tâche

Avantages clés

- Le pare-feu récompensé maintient les pirates et les logiciels malveillants éloignés. Les utilisateurs se sentent à l'abri lorsqu'ils sont en ligne. Le contrôle d'accès bidirectionnel signifie qu'une activité réseau non autorisée est impossible. La protection Ethernet spéciale protège les réseaux locaux contre les attaques par intermédiaires et les intrusions WiFi. Le composant Liste noire d'adresses IP bloquera la connectivité à des hôtes Internet prédéfinis, ce qui permettra à votre famille de rester loin des sites que vous considérez comme étant inappropriés.
- Le module Protection de l'hôte surveille le comportement et les interactions des programmes pour assurer une défense proactive contre les activités non autorisées, arrêter les chevaux de Troie, keyloggers et les rootkits dans leur sillage sans devoir rechercher les logiciels malveillants connus dans tous les objets suspects. La protection de l'hôte d'Outpost a atteint un taux de 100% d'efficacité dans les tests de fuite courants, ce qui assure une protection fiable contre les attaques de pirates inconnues et/ou sophistiquées.
- Le moteur d'analyse léger et très efficace associe un antivirus et un anti logiciels-espions pour détecter, désinfecter ou supprimer automatiquement les programmes malveillants. Le moniteur à l'accès est constamment sur ses gardes en cas de tentative malveillante pour entrer sur l'ordinateur ou pour l'activer. Son architecture souple lui assure une analyse très rapide en utilisant peu de ressources.
- Le module Web polyvalent garantit les activités de navigation des utilisateurs contre le côté sombre d'Internet en évitant les sites Web infectés de téléchargements accessoires, en empêchant la communication par inadvertance d'informations personnelles, en limitant l'exposition à des propriétés Web potentiellement peu sûres et en maintenant l'identité secrète.
- L'anti-spam avec fonction d'auto-apprentissage garde votre boîte de réception exempte de pourriels. Il s'améliore dès qu'il apprend à reconnaître ce que l'utilisateur considère comme du courriel non sollicité.
- La fonction d'autoprotection d'Outpost ne peut pas être désactivée par des attaques ciblées, assurant ainsi une protection ininterrompue.
- Grâce à un mécanisme évolué de journalisation des événements et à un nouveau mode d'affichage de l'activité des processus qui donne des informations détaillées sur tous les programmes actifs, les utilisateurs ont le nec plus ultra en matière de protection transparente pratique.

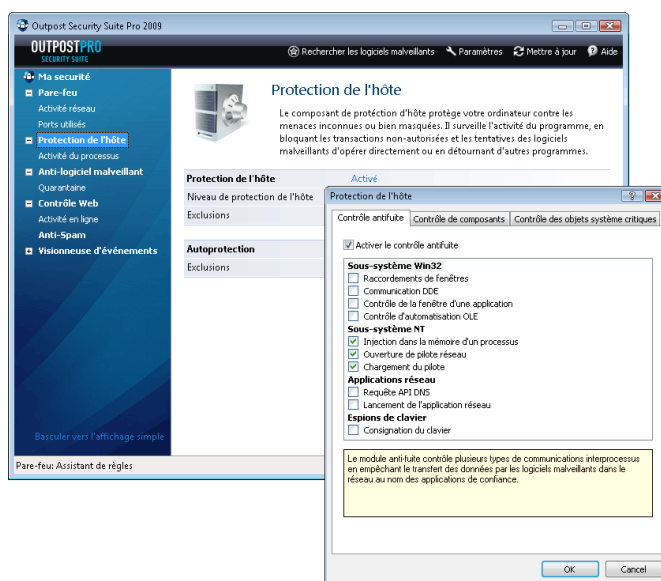
Outpost Security Suite Pro a été conçu pour répondre aux besoins des utilisateurs qui comprennent la nécessité d'une sécurité forte et efficace. Bien que proposant une grande protection dès son installation pour les utilisateurs de tous niveaux d'expérience, Outpost Security Suite Pro contient également une gamme complète de paramètres et d'options personnalisables pour les utilisateurs avancés qui pourront affiner et adapter leur protection. Les utilisateurs moins expérimentés pourront également bénéficier d'une bonne protection car Outpost leur permet de définir et d'appliquer la plupart des paramètres automatiquement, éliminant ainsi les potentielles erreurs de configuration. L'interface intuitive et les commandes accessibles garantissent une convivialité pour tout un chacun.

Fonctions clés

Sécurité proactive

Une protection préemptive contre les menaces

Outpost Security Suite Pro assure la première ligne de défense contre les logiciels malveillants en contrôlant de manière proactive le comportement et l'interaction entre programmes et évite toute brèche de sécurité. Le module Protection de l'hôte surveille et bloque de manière proactive les techniques de piratage sophistiquées employées pour compromettre ou dérober les données. En analysant les menaces et en affichant des alertes où vous pouvez intervenir, il bloque les attaques de type « zéro jour » et autres activités non autorisées, ce qui fournit une protection avancée contre les connexions zombies, les rootkits et la communication de données par imprudence. Cette dernière version accroît la portée des événements et des opérations surveillés pour une protection encore plus grande et plus personnalisable. Outpost excelle dans tous les tests d'étanchéité connus, avec une attention particulière portée aux activités d'enregistreurs de frappe.



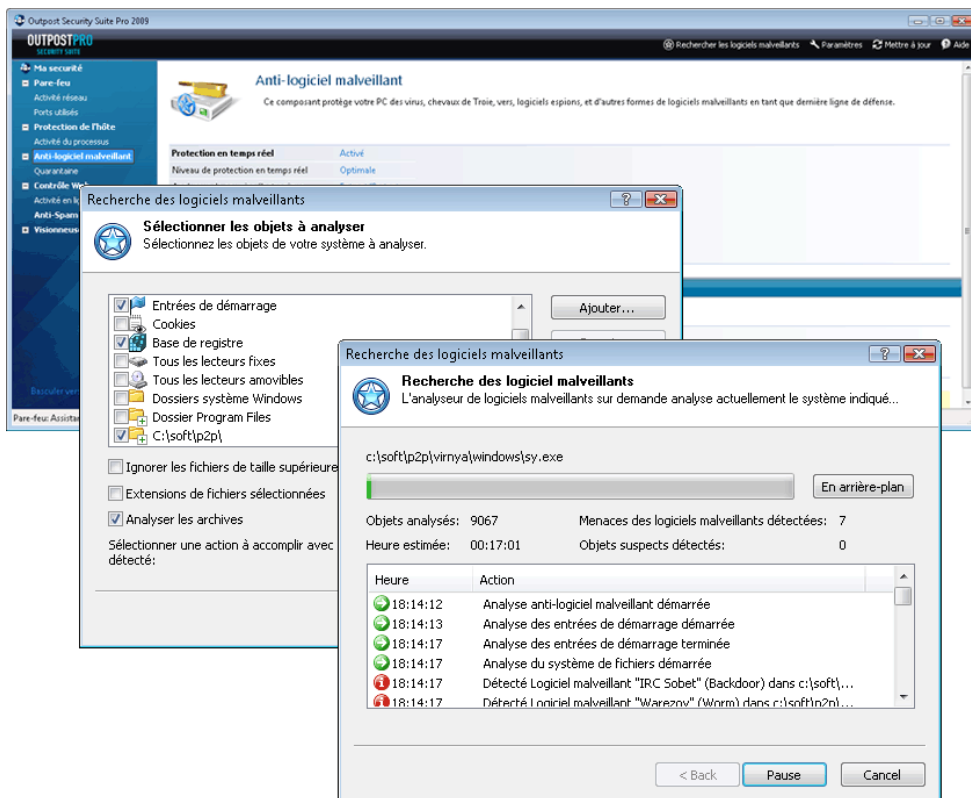
Autoprotection

Les logiciels malveillants recherchent fréquemment à couper les logiciels de sécurité afin de faciliter leurs processus d'infection. En incorporant pour tous ses composants une protection solide qui ne peut pas être modifiée sans accord, Outpost Security Suite Pro empêche quiconque à part de l'utilisateur du programme autorisé de désactiver ou de fermer la protection active.

Un anti logiciels malveillants efficace

Une protection à 360° contre les logiciels malveillants

Les fonction d'antivirus et d'anti logiciels-espions sont assurées par un module anti logiciels-espions universel qui garantit que l'ordinateur restera exempt de tout programme malveillant qui risquerait de l'infecter lorsque l'utilisateur est en ligne. Le moniteur à l'accès surveille continuellement et désinfecte, met en quarantaine ou supprime instantanément tout objet malveillant trouvé dans les zones clés de l'ordinateur alors que le scanner à la demande permet d'analyser les disques durs, dossiers réseau, DVD ou périphériques de stockage externes et d'en supprimer les menaces. Les pièces jointes aux courriels sont vérifiées en temps réel quand elles partent ou qu'elles arrivent. L'utilisateur peut déplacer tout fichier suspect vers la zone de quarantaine pour l'examiner ultérieurement. La protection supplémentaire empêche désormais les rootkits et autres logiciels malveillants élaborés de se charger et de s'incorporer sur l'ordinateur.



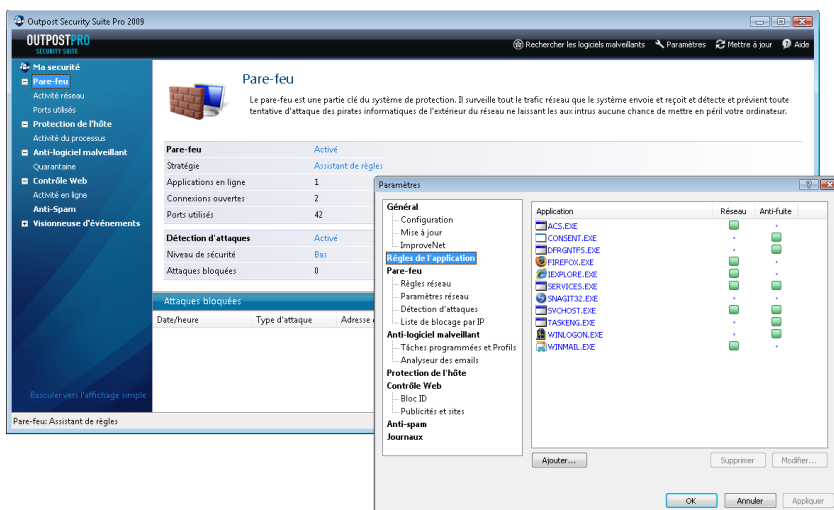
Analyses programmées et exclusions

Les utilisateurs peuvent définir une programmation souple pour les analyses de logiciels malveillants normales, mais également définir des critères d'analyse personnalisés comme la vérification des zones système critiques à chaque mise à jour des définitions de logiciels malveillants.

Sécurité et continuité réseau

Sécurité des connexions

Le pare-feu bidirectionnel surveille les connexions entrantes et sortantes sur l'ordinateur et empêche les accès au réseau non autorisés distants et locaux. Il cache les ports d'accès, ce qui rend la présence de l'utilisateur invisible sur Internet. Le module Protection Ethernet protège les connexions réseau et empêche les attaques depuis l'intérieur en contrôlant la transmission des données sur le réseau. Ceci élimine le risque potentiel pour les données comme les fenêtres de discussion ou les sessions de navigateur authentifiées d'être acheminées vers une mauvaise destination ou d'être interceptées en transit.



Contrôle de l'accès aux applications

Le pare-feu contrôle les programmes autorisés à accéder à Internet, ce qui protège de manière proactive l'ordinateur contre les menaces de type « zéro jour » et les tentatives de « phoning home » des logiciels malveillants.

Couverture complète

Outpost Security Suite Pro sécurise tous les types de connexion (Ethernet, WiFi, ADSL, câble, cellulaire et accès distant) en appliquant automatiquement les paramètres de sécurité nécessaires lorsque l'ordinateur est connecté à un nouveau fournisseur.

Protection contre l'intrusion

Le module Détection d'attaques empêche automatiquement les types d'attaque de piratage connus d'accéder à l'ordinateur.

Confidentialité et sécurité web

Protection contre les pourriels (spam)

Le moteur anti-spam avec filtre Bayes d'Outpost Security Suite Pro permettra d'avoir une boîte de réception sans courriel non sollicité. Les utilisateurs peuvent l'entraîner à reconnaître et à utiliser leur définition du pourriel. Plus ils l'utiliseront, plus il deviendra efficace et leur fera gagner de temps. L'anti-spam d'Outpost prend désormais totalement en charge le populaire client de messagerie The Bat!.

Limitation d'accès aux sites Web qui ne sont pas sûrs

Outpost peut facultativement vous avertir et bloquer l'accès à des sites Web potentiellement malveillants ou indésirables en fonction d'une liste prédéfinie d'URL. Ce filtrage assure aux utilisateurs de ne pas devenir la victime d'infections accessoires de logiciels malveillants ou d'hameçonnage cherchant à dérober leurs mots de passe, informations de connexion et autres données sensibles. La liste des sites bloqués est mise à jour via les mises à jour automatiques de l'anti logiciels-espions et peut être modifiée pour refléter les préférences de chacun.

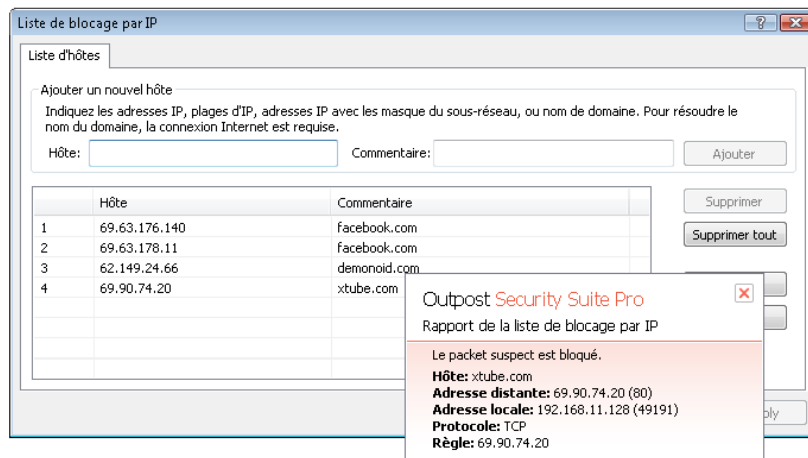


La liste noire d'adresses IP permet de surfer proprement

Basée sur le module BlockPost des anciennes versions d'Outpost, la liste noire d'adresses IP intégrée permet de limiter l'accès aux domaines Internet spécifiés. Outil très utile à la fois pour les parents soucieux et les personnes sensibles, la Liste noire d'adresses IP empêche les connexions

entrantes/sortantes vers des zones Internet mal intentionnées telles que celles qui diffusent des logiciels espions ou qui affichent des publicités et du spam graphique désagréables.

Les entrées bloquées peuvent être définies manuellement ou importées en tant que liste depuis des sources maintenues par la communauté.



Un référentiel sûr pour vos données personnelles

Toute information confidentielle (numéros de comptes bancaires et mots de passe, par exemple) que l'utilisateur définit au moyen de la fonction de blocage d'identité est bloquée et ne pourra pas quitter l'ordinateur par des voies de communication comme la messagerie instantanée, le Web ou les courriels. Le blocage d'identité protège contre le vol d'identité et les attaques d'hameçonnage qui ciblent vos données confidentielles personnelles. De plus, il s'assure que personne d'autre (même d'autres membres du foyer) ne pourra accidentellement ou délibérément communiquer ces informations sur Internet.

Un surf sans publicités et anonyme

En gérant les cookies et les URL de référence externes, Outpost permet de conserver un haut niveau de confidentialité lors de visites de sites d'achat, de loisirs ou d'actualités tout en autorisant les sites de confiance à collecter uniquement les informations nécessaires à la personnalisation des pages. En outre, Outpost Security Suite Pro permet aux utilisateurs de limiter les éléments affichés sur les pages Web, ce qui leur permet de bénéficier d'une navigation plus propre et plus rapide. Les utilisateurs peuvent également définir les sites autorisés ou non à afficher des images, faire défiler les bannières publicitaires, exécuter du code externe comme l'ActiveX ou les scripts Java, ou permettre les fenêtres intempestives. La dernière version d'Outpost assure même la compatibilité avec les sites Web les plus complexes et sophistiqués, ce qui vous offre un fonctionnement fluide et une plus grande sécurité lorsque vous êtes en ligne.

Suivi et contrôle

Surveillance des activités réseau

La surveillance des activités réseau d'Outpost affiche toutes les connexions que réalise l'ordinateur de l'utilisateur sur Internet ou le réseau local de façon à pouvoir voir ce qui se passe chaque fois et fermer rapidement toute connexion non autorisée. Dans la nouvelle version 2009, il est possible de grouper/dégrouper les connexions en fonction de l'application. Vous pouvez également rapidement modifier les règles existantes directement depuis l'interface.

Protection par mot de passe, plusieurs profils de configuration

Les utilisateurs peuvent définir des mots de passe pour protéger leur configuration contre les modifications accidentelles ou délibérées ainsi que créer et utiliser plusieurs profils de configuration pour

s'adapter au risque encouru. Pour les utilisateurs avancés, la possibilité de créer plusieurs points de restauration via la commande d'enregistrement/chargement de configuration est un grand « plus ».

Des journaux d'événements plus facilement gérables

Nouveau ! L'ancienne Visionneuse de journaux d'Outpost affichait l'historique des événements passés d'un ordinateur. La nouvelle version améliore la clarté et la maniabilité de la Visionneuse de journaux avec, de plus, la prise en charge de listes par catégorie qui peuvent être triées et filtrées selon différents critères définis par l'utilisateur.

Compatibilité

Homologation des pilotes et compatibilité avec les dernières plates-formes Windows

Nouveau! Outpost a reçu l'homologation WHQL (Windows Hardware Quality Labs), ce qui signifie que sa protection est conforme aux exigences rigoureuses de qualité, de compatibilité et de stabilité de Microsoft.

Règles de pare-feu adaptatives

Lors de déplacements avec un portable ou lors de changement de FAI, l'utilisateur n'a plus besoin d'ajuster manuellement sa sécurité en fonction des nouveaux paramètres de connexion : Outpost gère ceci automatiquement grâce à des paramètres propres aux connexions tels que les adresses DNS ou de serveur de passerelle sous la forme de variables d'environnement.

Mode divertissement pour des jeux et des vidéos sans interruption

Lorsque l'utilisateur joue à des jeux ou regarde des vidéos en plein écran sur son ordinateur, le mode Divertissement d'Outpost s'assure que le programme ne sera pas interrompu par des alertes s'il détecte de nouvelles activités. Les notifications de nouvelles activités sont gérées en tâche de fond sans sacrifier les niveaux de protection en cours. Les utilisateurs peuvent personnaliser les applications qui activeront automatiquement le mode Divertissement.

Convivialité et facilité d'emploi

Mode d'auto-apprentissage

Au premier démarrage d'Outpost, il fonctionne dans un mode spécial, le mode d'apprentissage, où toutes les notifications d'alertes sont supprimées. Pendant cette période, le programme fait silencieusement l'apprentissage de l'activité habituelle de l'utilisateur ainsi que des connexions surveillées par le pare-feu. Une fois la période d'apprentissage terminée, la Suite repasse en mode normal et vous demande une réponse uniquement lorsqu'une nouvelle activité est détectée, ce qui réduit spectaculairement le nombre d'alertes qui nécessitent votre intervention.

Configuration automatique

Les règles de la majorité des programmes qui accèdent à Internet sont appliquées automatiquement, ce qui ôte la saisie manuelle de règles chaque fois qu'une nouvelle application accède à Internet ou interagit avec un autre programme. Cela signifie que la plupart du temps, les utilisateurs n'ont pas à s'occuper des questions liées à l'accès à Internet, ce qui minimisera les interruptions et le risque d'exposition dus à des configurations insuffisamment sécurisées. Outpost contient une vaste gamme de stratégies d'accès prédéfinies. Ces paramètres peuvent être personnalisés à tout moment en fonction des besoins propres à chacun.

ImproveNet vous fournit des configurations davantage prêtes à l'emploi

ImproveNet est un système de configuration de consolidation et de distribution du programme sur la base du volontariat. Après avoir été étudiés et approuvés par les ingénieurs d'Agnitum, les résultats soumis par les utilisateurs d'Outpost sont distribués entre les utilisateurs, ce qui permet à tous les utilisateurs de bénéficier des règles les plus sûres et les plus à jour pour toute une gamme d'activités et d'applications.

Smartadvisor, l'aide contextuelle instantanée

Si ImproveNet n'a pas la réponse, SmartAdvisor est toujours à portée de main pour aider l'utilisateur à prendre la bonne décision lorsqu'il configure les informations d'accès d'une application.

Mises à jour automatiques

Chaque fois qu'une mise à jour d'Outpost Security Suite Pro paraît pendant votre période de licence, le module de mise à jour récupère automatiquement la dernière version sur le serveur d'Agnitum et l'applique dès qu'il y est autorisé.

Performances et optimisation

Des analyses plus rapides et plus intelligentes

SmartScan, le détecteur de fichiers intelligent, analyse uniquement les parties modifiées de votre système de fichier, ce qui évite les analyses répétées des fichiers qui n'ont pas changé depuis la dernière analyse. Le moteur anti logiciels malveillants rapide et intelligent n'a aucun impact sur les performances générales du système et peut fonctionner en tâche de fond pendant que vous travaillez. SmartScan a été davantage optimisé pour fournir des performances jusqu'à dix fois plus rapides lors de certaines opérations d'analyse et de vérification des flux de données.

Configuration requise

Plateformes prises en charge: Windows 32 et 64 bits (Vista, XP, Server 2003, 2008), Windows 2000 (SP3 et versions ultérieures).

Clients de messagerie pris en charge pour l'anti-spam: The Bat!, Windows Mail, Outlook Express, Outlook (toutes les versions).

Protocoles et services de messagerie pris en charge: POP3, SMTP, IMAP.

Configuration matérielle: Processeur à 450 MHz ou plus (x-86/x-64/multi-cœur), 256 Mo de RAM, 100 Mo d'espace libre sur le disque.