



Fiche technique

Outpost Network Security 3.2

Présentation

En ces temps économiques difficiles, les entreprises placent la fiabilité, l'efficacité et la rentabilité en tête de leur liste de courses lorsqu'elles recherchent une solution de sécurité. Outpost Network Security 3.2 (ONS 3.2) est un choix malin pour qui souhaite contrôler ses coûts tout en conservant une sécurité réseau robuste. Le faible coup unitaire, la simplicité de déploiement, de gestion et de configuration, le fonctionnement solide avec un impact minimal sur les ressources, la souplesse et les options de personnalisation associées à des technologies récompensées font d'ONS 3.2 la solution parfaite pour protéger les biens numériques de votre entreprise.

Grâce à Outpost Network Security 3.2, votre entreprise est protégée sur tous les fronts contre tous les types possibles de menace de sécurité : pirates, interruptions du fonctionnement et temps d'immobilisation, les virus et les logiciels malveillants, les attaques par Internet et par courriel, la perte de données ainsi que l'utilisation inappropriée d'Internet. Les capacités de gestion centralisée assurent une protection du point de terminaison conviviale et sans problème pour n'importe quelle entreprise disposant de ressources informatiques internes limitées.

Le challenge de la sécurité des PME

Une économie agitée amène avec elle une croissance exponentielle d'attaques ciblant les communications électroniques et autres données de valeur, ce qui force les entreprises à repenser la protection de leurs biens vitaux. La vulnérabilité des logiciels prépare le terrain aux attaques de logiciels malveillants de type « zéro jour » et aux brèches de données. Par conséquent, les entreprises doivent impérativement atténuer ces menaces avant que leur auteur ne soit en mesure de les exploiter. Parallèlement, le nombre de virus mutants et polymorphes qui ne peuvent pas être détectés au moyen des méthodes conventionnelles basées sur les signatures monte en flèche. Les rootkits et les chevaux de Troie sophistiqués nécessitent l'adoption de nouveaux mécanismes de réponse plus intelligents. Bien entendu, l'être humain demeure le seul et le plus gros point faible de toute infrastructure de sécurité. En effet, les utilisateurs visitent des sites Web qui ne conviennent pas, sortent de l'entreprise des données confidentielles sur des lecteurs USB et perdent ou vendent ce qu'ils contiennent. L'utilisation répandue et inappropriée des réseaux de convivialité, des vidéos en ligne et des sites de conversation font empirer la situation.

Alors que les utilisateurs sont occupés à mettre au défi les contrôles de sécurité au niveau du point de terminaison, les personnes qui doivent agir en tant qu'administrateurs informatique ou sécurité sont confrontés à la lourde tâche de maintenir les protections correctement configurées et à jour afin d'intercepter les dernières menaces en date. Même les entreprises équipées de deux douzaines d'ordinateurs ont besoin d'une méthode centralisée pour déployer, configurer et gérer la protection à distance sans devoir se rendre sur chacun des postes de travail ni avoir un diplôme en informatique.

La solution ONS 3.2

D'un coup d'œil

Outpost Network Security fonctionne en créant un environnement sécurisé sur l'ensemble du réseau, d'un point de terminaison au serveur et tout ce qui se trouve entre les deux. Ses outils de protection automatisés fonctionnent en arrière-plan sur les ordinateurs clients, protégeant ainsi les points de terminaison contre les dernières menaces et en s'assurant que les logiciels malveillants ne pourront pas se disséminer sur le réseau et au-delà. La protection des clients est déployée à partir d'une seule console d'administration accessible depuis n'importe quel ordinateur, ce qui permet à l'administrateur désigné de contrôler à distance la protection des postes de travail. La gestion de la configuration, l'exécution des tâches de protection et la mise à jour des logiciels clients peuvent être réalisées depuis un seul endroit.

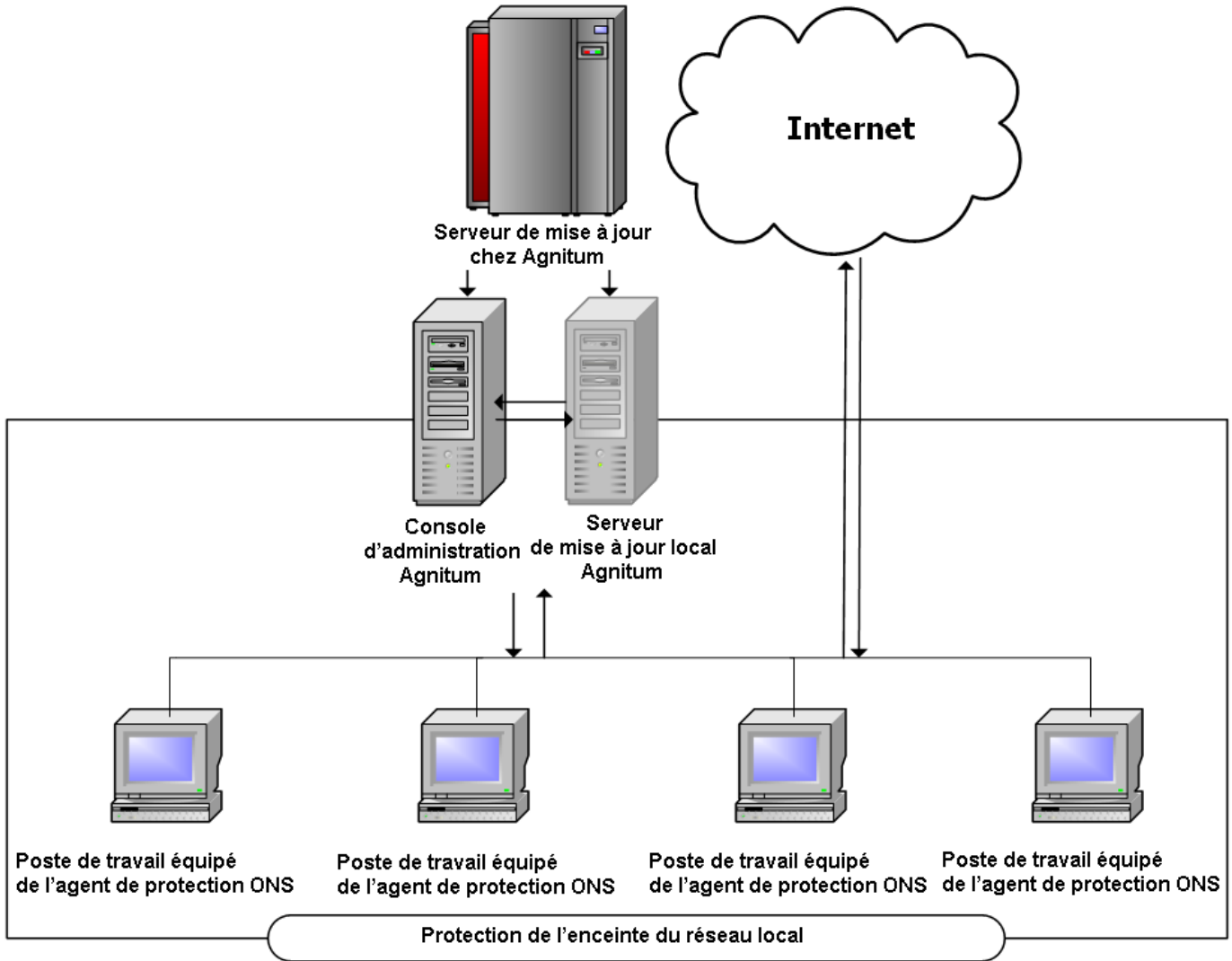
Outpost Network Security est le logiciel idéal pour les entreprises qui présentent les points suivants :

- réseaux de 5 à 500 ordinateurs ;
- employés mobiles, en déplacement ou télétravail ;
- plusieurs succursales ;
- budgets limités.

Principaux points de la protection ONS

- Le filtre antivirus et anti-logiciels espions automatisé contrôle la sécurité des points de terminaison en temps réel.
- Le scanner de sécurité à la demande recherche des logiciels malveillants sur les postes distants.
- Le pare-feu bidirectionnel surveille les connexions et protège contre les attaques réseau internes et externes.
- System Guard sécurise les emplacements systèmes critiques ainsi que le Registre, ce qui permet de garantir qu'aucune modification non autorisée ne sera apportée à ces zones vitales.
- Le système de blocage des périphériques USB garde les données de l'entreprise sous contrôle et empêche les fuites.
- Le contrôle Web permet de s'assurer que les utilisateurs ne pourront pas accéder à des sites Web dangereux ou interdits.
- L'autoprotection empêche les logiciels malveillants d'arrêter, sans autorisation, la protection du point de terminaison.
- Le moniteur de processus et d'activité réseau effectue le suivi en temps réel des événements distants.
- Les journaux distants vous permettent d'afficher les enregistrements passés dans un but d'audit.

Outpost Network Security 3.2 protège l'enceinte numérique de votre entreprise



Avantages d'Outpost Network Security 3.2

Aucun incident de sécurité

L'information est le bien le plus précieux de l'entreprise. Outpost assure l'intégrité de vos données en vous offrant des mécanismes de sécurité solides :

- **Un antivirus pour garantir un environnement sans logiciel malveillant**

Le moteur certifié VB100 qui associe une défense contre les virus et contre les logiciels espions est en permanence sur ses gardes pour détecter les logiciels malveillants qui apparaissent en interne (c'est-à-dire reçus en pièce jointe à un courriel) ou captés à l'extérieur (qui se répandent via un lecteur flash USB contaminé). La menace est neutralisée instantanément avant qu'elle ne puisse mettre en danger d'autres ordinateurs membres du réseau. Les analyses antivirus à la demande distantes et centralisées peuvent être lancées à tout moment sur des points de terminaison sélectionnés.

- **Pare-feu bidirectionnel pour renforcer la connexion LAN**

La technologie de pare-feu récompensée permet de garantir la sécurité et la continuité de fonctionnement du réseau de votre entreprise. Grâce à un système de détection des intrusions unique empêchant toute écoute, grâce au filtrage des paquets et des applications pour bloquer les connexions non souhaitées ou malveillantes ou encore grâce à la protection de code incorporée pour consolider les éléments Web vulnérables, Outpost Network Security constitue l'arme ultime dans tous les cas où vos informations courent un danger et où les pirates vous attaquent.

- **System Guard**

System Guard permet à l'administrateur de définir la liste des programmes protégés sur le système, de même que le grand nombre de paramètres et de fichiers de configuration de Windows. Il peut s'agir, notamment, des paramètres du Registre, les propriétés de mise en réseau, l'accessibilité aux fichiers hôte, les interactions des plug-ins Adobe Flash et Reader et autres objets vulnérables aux attaques. Tout programme désigné est protégé contre la modification ou la mise en danger non autorisée par System Guard.

- **Contrôle Web**

Les administrateurs peuvent configurer les points de terminaison pour bloquer de façon proactive l'accès à des pages Web non autorisées en fonction de mots-clés inclus dans l'adresse URL ou dans le corps de la page.

- **Verrouillage de l'accès USB pour protéger les biens numériques de l'entreprise**

Vos données internes courent le risque d'être copiées et de sortir de votre entreprise. Outpost Network Security bloque l'accès aux périphériques de stockage de masse USB sur les hôtes cibles, empêchant ainsi la fuite non autorisée des données de l'entreprise et la propagation des logiciels malveillants à partir des lecteurs de mémoire flash connectés.

Installation sans effort et mises à jour automatiques

- **Déploiement centralisé pour réduire la charge du service Informatique**

Le déploiement de masse peut être réalisé en très peu de temps grâce à des outils intuitifs établissant la cartographie du réseau de l'entreprise.

- **Mises à jour en ligne et hors ligne pour une protection à jour**

Les mises à jour de sécurité pour les ordinateurs reliés à l'intranet sont déployées quotidiennement à partir d'un simple référentiel réseau tel qu'un serveur Agnitum, un serveur de mises à jour local ou un dossier local contenant des bases mises à jour.

Gestion et configuration centralisées

- **Segmentation en groupes pour une protection plus ciblée**

Les ordinateurs connectés peuvent être divisés en groupes, chaque groupe possédant ses propres propriétés de sécurité. Ceci permet de mieux gérer et cibler les destinataires de la protection, de même qu'affecter des stratégies plus résistantes à des groupes plus fragiles (comme un groupe d'utilisateurs mobiles).

- **Configuration à distance pour une gestion facile et pratique**

Dans la nouvelle version d'Outpost Network Security, il est possible de gérer les ordinateurs reliés ensemble à partir d'un poste de travail quelconque via une console d'administration universelle. Les administrateurs peuvent stipuler des règles d'accès à Internet personnalisées et indiquer une liste noire d'adresses URL qui ne seront pas accessibles depuis le réseau.

Meilleure visibilité des événements distants

- **Contrôle en temps réel de l'activité des points de terminaison pour une transparence totale**

Une fois que votre réseau est en état de fonctionner, il est difficile de contrôler les événements qui se passent sur chaque ordinateur. Outpost contourne ce problème en proposant la surveillance du système et des activités réseau en temps réel pour n'importe quel hôte distant.

- **Système de connexion à distance pour une meilleure compréhension des activités passées**

Le dispositif de connexion à distance d'Outpost affiche l'historique de tous les événements passés qui se sont déroulés sur les ordinateurs distants, ce qui permet aux gestionnaires informatiques de trouver rapidement un problème et de le résoudre sans quitter leur bureau.

Protection légère permanente

- **Utilisation plus rapide grâce à SmartScan**

Grâce à de nombreuses optimisations et à des technologies uniques d'accroissement des performances, la protection Outpost cliente a lieu en tâche de fond sans accaparer des ressources système vitales. Les vérifications de sécurité sont dix fois plus rapides que celles de nos concurrents.

- **Prévention de l'arrêt non autorisé pour garantir la continuité de la protection**

Il est impossible de désactiver la protection Outpost des postes de travail dans le cas d'attaques dans ce but, ce qui signifie que vos clients en réseau demeurent protégés 24h sur 24/7j sur 7.

Compatibilité universelle

- **Prise en charge des matériels et logiciels modernes pour un déploiement plus étendu**

ONS 3.2 propose une prise en charge optimale pour toutes les plateformes Windows actuelles 32 et 64 bits, notamment Windows 7, Windows Vista SP2, Windows Server 2008 et Windows Server 2008 R2.

Fonctionnalités d'Outpost Network Security 3.2

Sécurité et confidentialité des données

- **Protection puissante contre les logiciels malveillants**

Outpost Network Security fournit une protection complète contre toutes les formes de menace de logiciels malveillants, notamment les virus, les logiciels espions, les chevaux de Troie et les vers. Il protégera les postes de travail de votre entreprise 24 heures/24, 7 jours/7, quel que soit le niveau d'expérience de l'utilisateur. Nouveau ! Le système d'analyse automatisé en fond empêche les infections par des logiciels malveillants en temps réel, alors que le scanner à la demande centralisé utilise la technologie unique SmartScan 3 d'Agnitum pour assurer la détection et la désinfection rapides et efficaces de tous les systèmes de stockage (local, distant et partagé). L'administrateur informatique peut lancer une analyse distante arbitraire sur le poste de travail qu'il choisira (tant que la console d'administration y sera installée). Les ordinateurs de l'entreprise seront vérifiés afin d'y rechercher de nouvelles infections à intervalle régulier via la fonction d'analyse programmée. Les signatures de menaces mises à jour sont distribuées quotidiennement via un point désigné de votre réseau (le serveur Agnitum, le serveur de mises à jour local ou un dossier local possédant des bases de données mises à jour).

- **Continuité du fonctionnement du réseau**

Le pare-feu ONS orienté client protège les connexions réseau entrantes et sortantes, il filtre l'ensemble du trafic en fonction des stratégies d'accès définies par l'administrateur et en bloquant les transmissions non souhaitées ou malveillantes. Une protection Ethernet unique vous protège contre les attaques de type « man-in-the-middle » conçues pour intercepter les données du réseau, vous assurant ainsi que les données en transit atteindront toujours leur destinataire.

- **System Guard**

Le System Guard sécurise les emplacements systèmes critiques ainsi que le Registre, ce qui permet de garantir qu'aucune modification non autorisée ne sera apportée à ces zones vitales. System Guard permet à l'administrateur de définir la liste des programmes protégés sur le système, de même que le grand nombre de paramètres et de fichiers de configuration de Windows. Il peut s'agir, notamment, des paramètres du Registre, les propriétés de mise en réseau, l'accessibilité aux fichiers hôte, les interactions des plug-ins Adobe Flash et Reader et autres objets vulnérables aux attaques.

- **Verrouillage des périphériques USB**

Pour empêcher toute propagation de logiciels malveillants à partir de sources externes de même que la copie non autorisée de données propres à l'activité, les entreprises peuvent mettre en place des restrictions d'utilisation de périphériques de stockage USB pour certains employés.

- **Sécurité Web**

Aujourd'hui, le Web constitue la source n°1 des menaces de sécurité des entreprises. Outpost Network Security permet à votre productivité de rester à son maximum et réduit les risques en limitant la quantité de contenus Web pouvant être exécutée ou affichée sur chaque poste de travail. Du blocage des scripts dangereux jusqu'à la

suppression des illustrations Web inutiles, des animations et des bandeaux publicitaires, ONS empêche tout téléchargement accessoire et autres attaques furtives en provenance du Web. En outre, les gestionnaires peuvent bloquer l'accès à certains domaines Internet dangereux en fonction de l'utilisateur.

- **L'auto-défense assure une protection 24h sur 24**

ONS est équipé d'une technologie d'auto-défense visant à bloquer les tentatives d'arrêt de la protection par des tiers non autorisés, ceci afin de conserver une protection sans interruption.

Contrôle et maniabilité

- **Déploiement et administration centralisés**

La protection cliente est déployée depuis une console d'administration centrale en sélectionnant simplement les destinataires cibles. En quelques minutes seulement, tous les points de terminaison indiqués sont protégés. Toutes les procédures d'administration suivantes pourront être gérées à partir d'un poste de travail sur le réseau.

- **Segmentation du groupe des utilisateurs**

La prise en charge de groupes d'utilisateurs permet le déploiement de différentes configurations et règles d'accès pour différents utilisateurs selon leur niveau de risque.

- **Visibilité détaillée des événements distants**

D'une façon tout à fait unique, ONS permet à l'administrateur de contrôler les événements sur un ordinateur distant en temps réel. Les rapports d'activités comportent des informations telles que les programmes et les processus actifs, les adresses réseaux auxquelles les utilisateurs accèdent et autres statistiques pertinentes.

- **Gestionnaire des événements complet**

Grâce à la journalisation détaillée des activités passées des points de terminaison, les administrateurs peuvent facilement trouver et réparer les problèmes de connexion, afficher le statut de la suppression des logiciels malveillants et accéder à d'autres informations liées à la maintenance du réseau.

Configuration requise pour Outpost Network Security 3.2 :

Plateformes prises en charge :

ONS 3.2 propose une prise en charge optimale pour toutes les plateformes Windows actuelles 32 et 64 bits, notamment Windows 7, Windows Vista SP2, Windows Server 2008 et Windows Server 2008 R2.

Matériel :

Processeur à 500 MHz ou plus (x86/x64/multi-cœur), 256 Mo de RAM, 100 Mo d'espace libre sur le disque.

Améliorations de la version Outpost Network Security 3.2

Version du produit	Outpost Office Firewall	Outpost Network Security 2.0	Outpost Network Security 3.0	Outpost Network Security 3.2
Le pare-feu for protéger les connexions des points de terminaison	oui	oui	oui	oui
Anti logiciel espion pour la protection élémentaire contre les logiciels malveillants	oui	oui	oui	oui
Antivirus pour une protection totale contre les logiciels malveillants	non	non	oui	oui
System Guard (sécurise les emplacements systèmes critiques ainsi que le Registre)	non	non	non	oui
Déploiement simplifié via l'installation en nuage	non	non	oui	oui
Scans anti logiciels malveillants exécutables à la demande et à distance	non	non	oui	oui
Verrouillage de l'accès aux périphériques de stockage USB	non	non	oui	oui
Contrôle Web	non	non	non	oui
URL sur liste noire gérées de façon centralisées	non	non	oui	oui
Segmentation des groupes d'utilisateurs pour une protection plus ciblée	non	oui	oui	oui
Affichage distant des journaux des événements passés	non	non	oui	oui
Surveillance en temps réel de l'activité des points de terminaison	non	non	oui	oui
Prise en charge de la console d'administration/agent client pour Windows 7 et Server 2008 R2	non	non	non	oui

Essayez-le !

Pour constater vous-mêmes combien il est facile de protéger votre PME contre les menaces d'aujourd'hui et de demain, rendez-vous à l'adresse <http://www.agnitum.com/products/networksecurity/index.php> et téléchargez une version d'évaluation de 30 jours entièrement fonctionnelle d'ONS 3.2.