AppSense Application Manager
Fiche produit

Équilibre pratique et économique entre la conformité IT et la demande des utilisateurs

Fonctions principales:

- Droit contextuel de l'application
- Analyse du périphérique
- Contrôle d'accès réseau aux applications
- Contrôle des licences logicielles
- Supervision en mode passif
- Audit intégré des événements
- Redirection URL
- Arrêt des applications

Principaux avantages:

- Maintient l'environnement dans l'état souhaité
- Accroît la visibilité du paysage applicatif
- Applique le licensing, garantit la conformité
- Réduit les appels au support
- Favorise l'adoption des utilisateurs

À propos d'AppSense

AppSense est le fournisseur leader de solutions de gestion de l'environnement utilisateur pour les entreprises, favorisant la productivité et la sécurité des utilisateurs dans des environnements de travail à la fois fixes et mobiles. La suite AppSense de gestion de l'environnement utilisateur a été déployée par plus de 3.000 clients dans le monde, et permet d'administrer plus de 6 millions de terminaux. Nos solutions, comprenant DesktopNow, MobileNow et DataNow, réduisent la complexité de l'administration IT, et améliorent le déploiement et la gestion des périphériques, des applications et des données au sein de l'entreprise. La société est basée à Sunnyvale, en Californie, et possède des bureaux dans le monde entier. Pour en savoir plus sur nos solutions IT, rendez-vous sur appsense.fr

Droit de l'application utilisateur

Que ce soit un environnement utilisateur fourni via le réseau central ou via les bureaux physiques ou virtuels, ou toute combinaison de ceux-ci, il est essentiel que les utilisateurs n'aient accès qu'aux seules applications dont ils ont besoin et qu'ils ne puissent introduire des exécutables inconnus dans l'environnement.

L'utilisation de logiciels non autorisés est un des principaux facteurs de déstabilisation des environnements utilisateurs et les coûts associés à la remise en état d'un poste de travail corrompu peuvent être élevés. Dans un environnement utilisateur partagé tel que sur un réseau central, ces coûts sont aggravés lorsque l'action d'un utilisateur a des répercussions sur de nombreux autres utilisateurs. Les méthodes actuelles pour faire respecter l'utilisation des applications se limitent à des scripts complexes ou à l'entretien rigoureux de listes blanches ou noires.

Trusted Ownership™

Grâce aux pilotes de filtrage sécurisés au niveau du noyau et aux politiques de sécurité NTFS de Microsoft, AppSense Application Manager intercepte toutes les demandes d'exécution et bloque toutes les applications indésirables. Le droit des applications est basé sur la propriété de l'application, celle-ci étant attribuée par défaut à l'administrateur. En utilisant cette méthode, la politique actuelle d'accès aux applications est exécutée dès la première utilisation sans qu'il n'y ait besoin de gérer de script ou de listes. Cette méthode est appelée Trusted Ownership™. Outre les fichiers exécutables, AppSense Application Manager gère également le droit d'un contenu d'application tel que les contrôles ActiveX, les VBScripts, les fichiers batch, les paquets MSI et les fichiers de configuration du registre.

L'élévation de privilèges

Les droits utilisateur sont contrôlés de manière dynamique avec une précision chirurgicale. Les utilisateurs ne disposent que des droits administrateur dont ils ont besoin pour exécuter une application, ce qui permet de contenir les coûts liés au support. La solution ne consiste pas à contrôler les droits utilisateur au niveau de la session ou du compte mais au niveau de l'application ou d'une tâche individuelle. Les droits peuvent être supprimés ou restreints en fonction de l'utilisateur, de l'application ou de la tâche.

Pas seulement les applications

En plus des applications, AppSense Application Manager assure la gestion par les droits, des demandes de connexion sortantes vers les chemins UNC et les URL et fournit ainsi une seule solution à toutes les règles d'admissibilité des applications et du réseau. Les connexions, les URL et les applications peuvent également être interrompues en fonction de règles.

Droit contextuel

Le degré d'accès d'un salarié aux applications de l'entreprise peut dépendre du contexte du périphérique de connexion. Par exemple, un utilisateur dans un cybercafé, n'aura pas le même niveau d'accès aux applications qu'un employé connecté au réseau local sécurisé de l'entreprise. AppSense Application Manager est capable d'exploiter les informations relatives au contexte de l'utilisateur pour déterminer le niveau de droit nécessaire. Des paramètres tels que l'emplacement, les paramètres de pare-feu et même le moment de la journée peuvent être utilisés pour établir un niveau de droit nécessaire.

Droit hors ligne

Les employés étant de plus en plus mobiles, il est impératif que les règles d'admissibilité soient appliquées lorsque l'utilisateur n'est pas connecté au réseau de l'entreprise. AppSense Application Management veille également à ce que les employés accèdent aux applications et aux ressources pour lesquelles ils ont l'autorisation d'accès lorsqu'ils sont hors ligne.

Gestion des licences

AppSense Application Manager est reconnu par Microsoft ® pour appliquer un dispositif de contrôle des licences logicielles. L'exécution du logiciel en mode passif permet la supervision, l'audit et le reporting afin de détailler la fréquence d'accès aux applications pour chacun des utilisateurs et selon le périphérique. Le contrôle des utilisateurs ou des équipements autorisés à exécuter certaines applications précises, permet d'établir des limites sur le nombre d'instances d'application, sur les équipements et les utilisateurs autorisés à exécuter l'application, sur le moment où les utilisateurs exécutent un programme et sa durée d'utilisation. Les audits de licence et les restrictions d'accès basés sur le nombre de licences peuvent désormais être appliqués indépendamment de la méthode de distribution des applications. Cet audit de licence peut également être utilisé dans vos environnements de bureaux virtuels et physiques.

AppSense Application Manager
Fiche produit

appsense.fr
iwanttoknowmore@appsense.com

Caractéristiques d'AppSense Application Manager:

Trusted Ownership™

Il n'est pas nécessaire d'utiliser des listes complexes et de gérer en permanence pour protéger le système. Seul le code installé et détenu par les « propriétaires de confiance » est autorisé à s'exécuter. La liste des propriétaires de confiance peut être étendue pour répondre à tout type d'environnement ou d'infrastructure de répertoire de contenu.

Gestion des droits utilisateur

Le niveau de privilège d'un utilisateur, d'un groupe ou d'un rôle peut être élevé ou réduit pour les applications et les applets du panneau de commande. Les comptes d'admin locaux peuvent être supprimés et pourtant les utilisateurs peuvent toujours accéder à certaines applications ou tâches qui nécessitent des droits d'administrateur.

Analyse du périphérique

Identifiez tous les fichiers exécutables sur un périphérique cible et regroupez les fichiers en fichiers autorisés et non autorisés pour créer rapidement une politique. Les configurations peuvent être déployées pour un utilisateur, un groupe d'utilisateurs, une machine ou un groupe de machines. En quelques minutes, le droit de l'application va automatiquement contrôler l'utilisation des applications.

Analyse de l'utilisation des applications

Analysez un périphérique cible et identifiez le nombre de fois où les applications individuelles ont été exécutées par un utilisateur. En mettant en évidence les applications qui sont utilisées et celles qui ne le sont pas, les logiciels sans licence ou inutilisés peuvent être identifiés et limités et les logiciels sous licence peuvent être retirés, ce qui réduit à la fois la quantité d'applications sur un périphérique et le coût des licences pour ces applications.

Supervision passive

Supervisez l'utilisation des applications sans empêcher les utilisateurs d'exécuter ces dernières. La supervision passive peut être activée ou désactivée sur la base d'un utilisateur, d'un périphérique ou d'un groupe et représente un outil bien utile pour suivre avec précision le comportement des utilisateurs avant une implémentation complète ou pour comprendre l'utilisation des applications dans le cadre de la gestion des licences logicielles.

Configurations des listes blanches et noires

Les configurations de listes blanches et noires peuvent être utilisées avec Trusted Ownership pour contrôler les applications connues qui réussissent la vérification de propriété NTFS. Les applications auxquelles les utilisateurs ne devraient pas avoir accès tels que les outils détenus par l'administrateur (par ex. cmd.exe ou ftp.exe) sont automatiquement refusées. Vous pouvez également créer des listes blanches pour garantir l'exécution des applications connues et de confiance sur un système.

Signatures numériques

Attribuez des signatures numériques SHA-1 aux applications et aux fichiers afin de garantir leur intégrité. Les applications modifiées ou falsifiées ne s'exécutent pas.

Contrôle d'accès réseau aux applications

Contrôlez l'accès au réseau sans contrôles complexes tels que les routeurs, les switches et les pare-feu. Les connexions sortantes d'un périphérique cible sont soumises à des règles d'admissibilité.

Les connexions comprennent l'accès à des chemins UNC (y compris tous les fichiers et dossiers présents sur ce disque), à des serveurs, à des adresses IP, à des URL, à des périphériques et à des sites FTP. La politique peut être adaptée pour être modifiée dynamiquement en fonction de l'utilisateur ou des propriétés du périphérique.

Utilisateurs auto-autorisés

Autorisez certains utilisateurs nommés à exécuter des applications qu'ils ont introduites dans le système. Les applications peuvent être ajoutées à une machine sécurisée en dehors du bureau sans avoir recours à l'assistance informatique. Un audit complet détaille des informations telles que le nom de l'application, l'heure et la date de l'exécution et le périphérique. De plus, une copie de l'application peut être prise et stockée de manière centralisée en vue d'une analyse.

Droits d'installation des applications au niveau du Web

Contrôlez une « liste blanche » de sites Web approuvés à partir desquels les utilisateurs sont autorisés à installer des logiciels. Par exemple, des sites connus tels que www.adobe.com et www.gotomeeting.com. Les utilisateurs peuvent ainsi accéder aux applications d'entreprise telles qu'Adobe Reader, Adobe Air, Adobe Flash Player et au client de web conférence GoToMeeting sans impacter la distribution des applications informatiques.

Droits d'installation des applications au niveau de l'application

En plus des droits d'installation au niveau des sites Web, certaines entreprises peuvent exiger un contrôle plus précis des applications que les utilisateurs installent à partir de sites Web spécifiquement approuvés. Pour reprendre l'exemple précédent, un administrateur IT peut souhaiter autoriser l'installation d'Adobe Reader mais bloquer Adobe Air, Adobe Flash Player et/ou toutes les autres applications de www.adobe.com. Contrôlez par liste blanche les applications spécifiques par version et par contrôle ActiveX de la catégorie sur le site Web en question si nécessaire. Cela garantit que seules les versions de confiance de ces applications spécifiques peuvent être installées depuis le Web par les utilisateurs.

Limitations sur les applications et restrictions de temps

Appliquez une politique pour contrôler le nombre d'instances d'application qu'un utilisateur peut exécuter, ainsi que le moment de son exécution. Une politique peut être créée pour contrôler ou exécuter des modèles de licences en contrôlant les limites de l'application par périphérique.

Redirection d'URL

Lorsqu'un navigateur web est laissé ouvert, soit sur une page web soit sur une application web, et si l'utilisateur se reconnecte à partir d'un nouvel appareil ou d'un nouvel emplacement, le navigateur peut être redirigé vers une adresse sécurisée et prédéfinie. Des variables peuvent être définies en ce qui concerne le moment de la redirection, et des règles peuvent être établies pour les URL qui doivent être interdites et/ou redirigées.

Prise en charge étendue de fichiers

Outre le contrôle des applications telles que les fichiers .exe, les fichiers de script, de batch et de registre sont également contrôlés. Des signatures numériques peuvent aussi être appliquées à des scripts pour s'assurer que le contenu reste inchangé.

Modèles de configuration AppSense

Tirez profit des meilleures pratiques préétablies de politique d'entreprise en important les modèles de configuration AppSense. AppSense Application Manager est en mesure d'importer un nombre illimité de fichiers de configuration et d'utiliser celles-ci en combinaison. Une sélection de modèles de configuration tels que « éléments fréquemment interdits » ou « Analyse du périphérique » est disponible à l'adresse www.myappsense.com. Cette bibliothèque de modèles est maintenue à jour en permanence.

Mode découverte des droits utilisateur

Analysez rapidement et faites état de dizaines de milliers de postes de travail, identifiez les applications et les tâches nécessitant des droits d'administrateur. Les options de rapports flexibles permettent d'ajouter très facilement les résultats à une configuration.