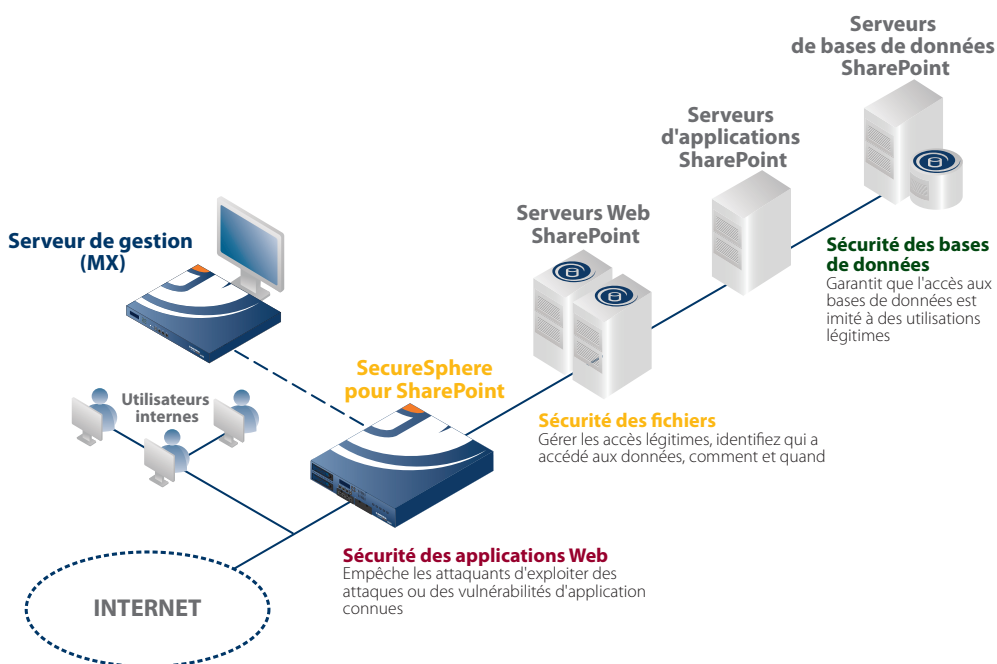


SecureSphere pour SharePoint

Sécurité des données pour les fichiers SharePoint, les ressources Web et les bases de données

SecureSphere pour SharePoint aide les entreprises à protéger les données sensibles stockées dans Microsoft SharePoint. Il répond aux exigences de sécurité des fichiers SharePoint, des éléments Web et des bases de données, assurant ainsi que les utilisateurs dont les besoins sont légitimes puissent accéder aux données et que les autres ne le puissent pas. SecureSphere pour SharePoint assure la visibilité et l'analyse des droits d'accès et d'utilisation des données, et la protection contre les menaces provenant du Web.

SecureSphere pour SharePoint assure une sécurité multi-couches qui inclut un Firewall applicatif Web destiné à protéger contre les attaques émanant du Web, la gestion des droits des utilisateurs et la surveillance de l'activité afin de protéger les contenus comme les fichiers, les dossiers et les listes, et un pare-feu pour bases de données destiné à empêcher tout accès non autorisé à la base de données Microsoft SQL au cœur de SharePoint.



Avantages de SecureSphere pour SharePoint

Opérations IT

- » Gestion simultanée des permissions et des révisions des droits des utilisateurs
- » Décidez de la meilleure méthode pour gérer les données
- » Trouvez des données perdues, manquantes ou supprimées
- » Libérez un précieux espace de stockage

Sécurité

- » Assurez-vous que les accès sont basés sur des besoins légitimes
- » Documentez la conformité, menez des enquêtes poussées et isolez les modifications
- » Faites respecter les règles de l'entreprise
- » Déterminez comment gérer et protéger au mieux les données
- » Protégez-vous des attaques émanant du Web
- » Empêchez que la base de données Microsoft SQL de SharePoint ne soit sciemment modifiée
- » Sécurité rapidement assurée

Regrouper les permissions SharePoint et créer des reports

SecureSphere regroupe et consolide les droits des utilisateurs sur l'ensemble des sites SharePoint afin d'assurer la visibilité requise sur les permissions effectives. Avec SecureSphere pour SharePoint, les entreprises peuvent valider les droits, éliminer les droits excessifs, et identifier les utilisateurs inactifs, ceci contribuant à ce que les accès soient basés sur des besoins légitimes.

Procéder à l'audit de toutes les activités d'accès aux données

SecureSphere assure la surveillance permanente et l'audit détaillé de toutes les activités d'accès aux données afin que les entreprises possèdent un audit complet montrant le « Qui, Quoi, Quand, Où et Comment » de chaque accès aux données. Ceci permet au personnel de sécurité, de conformité et d'administration de SharePoint de comprendre exactement qui a accédé, déplacé, modifié ou supprimé des données.

Appliquer les règles de sécurité en temps réel

SecureSphere pour SharePoint assure un cadre de règles flexibles permettant à l'entreprise de réagir immédiatement lorsque l'activité d'accès aux données s'écarte de la politique d'entreprise. Des alertes sont générées dans la console SecureSphere et peuvent aussi entraîner des actions externes telles que l'envoi d'un e-mail ou le blocage de l'accès aux données.

Identifier les propriétaires des données

SecureSphere contribue à identifier les propriétaires des données en assurant la visibilité des principaux utilisateurs des fichiers, dossiers et listes SharePoint. Les propriétaires comprennent l'importance de leurs données et apportent une contribution critique sur la façon dont ces données doivent être gérées et protégées.

Découvrez Imperva

Imperva est le leader mondial de la sécurité des données

Des milliers d'entreprises de premier plan dans le monde, d'organismes gouvernementaux et de fournisseurs de services s'appuient sur les solutions Imperva pour prévenir les fuites de données, répondre aux exigences de conformité et gérer les risques menaçant les données. Soulignant l'engagement d'excellence d'Imperva dans la sécurité des données, le centre de défense des applications d'Imperva (Application Defense Center, ADC) est un organisme de recherche de niveau mondial qui maintient la protection de pointe SecureSphere à l'encontre des menaces grandissantes.

Imperva France SARL
4 place de la Défense
La Défense 4
92974 Paris La Défense Cedex
France
Tel: +33 1 70 15 07 99

www.imperva.com

© Copyright 2011, Imperva

Tous droits réservés. Imperva, SecureSphere et "Protecting the Data That Drives Business" sont des marques commerciales enregistrées par Imperva. L'ensemble des autres marques ou noms de produits sont des marques commerciales déposées ou enregistrées par leurs titulaires respectifs.

#DS_SS_SHAREPOINT-A4-FR-0911rev1

Protégez-vous des attaques émanant du Web

SharePoint est un système basé sur le Web, sujet à des attaques en ligne telles que SQL injections et Cross-site Scripting (XSS). SecureSphere pour SharePoint inclut le Firewall pour applications Web SecureSphere leader du marché, qui protège SharePoint des menaces de sécurité actuelles et futures émanant du Web.

Empêcher tout accès non autorisé aux bases de données

SharePoint stocke toutes les données – fichiers, listes et données d'application – dans une base de données Microsoft SQL. SecureSphere pour SharePoint incorpore le pare-feu pour bases de données SecureSphere leader du marché afin de surveiller tous les accès aux bases de données et s'assurer que tout accès non autorisé est empêché.

Identifier les données inutilisées

SecureSphere aide à limiter la croissance permanente des données SharePoint en identifiant celles qui sont stockées dans SharePoint, mais que personne n'utilise. Ceci permet aux entreprises d'archiver ou de supprimer ces données, réduisant ainsi les coûts de gestion et libérant un précieux espace de stockage.

Sécuriser SharePoint rapidement

SecureSphere pour SharePoint inclut des règles de sécurité prédéfinies basées sur l'expertise des chercheurs en sécurité du centre de défense des applications (Application Defense Center, ADC) d'Imperva. Les connaissances d'ADC pour SharePoint aident les entreprises à sécuriser rapidement leurs déploiements SharePoint.

