

SecureSphere®

Passerelle de sécurité de base de données

Pertinence fonctionnelle, haute
sécurité, efficacité opérationnelle



La sécurité des bases de données est l'une des demandes les plus exigeantes du paysage IT. Abus de privilèges et intrusion, infection de vers, attaques d'applications constituent des menaces constantes. Les nouvelles obligations réglementaires concernent les processus étendus d'évaluation, de contrôle et d'audit requis pour les bases de données et applications métiers. Tous ces processus doivent être mis en œuvre dans un environnement de centre de données qui supporte de nombreux privilèges utilisateur en changement constant, des taux de transaction élevés, et des exigences de disponibilité strictes.

La passerelle SecureSphere répond aux exigences de sécurité des bases de données. Les politiques en profondeur de la sécurité des bases de données détectent toute l'envergure des attaques avec une extrême précision. Le déploiement transparent, le profilage utilisateur adaptatif, la haute disponibilité souple, et les capacités de performance multi-gigabits garantissent une efficacité opérationnelle inégalée. De plus, le contenu des services optionnels ADC Insight élimine le temps passé à rechercher les détails de l'audit et des pratiques de sécurité liées aux réglementations spécifiques et applications métier.

La passerelle SecureSphere

La passerelle de sécurité de bases de données SecureSphere® permet le contrôle automatisé de l'activité, l'audit et la protection des bases de données Oracle, MS-SQL, IBM DB2 (y compris gros systèmes), Sybase, et Informix.

La technologie du Profilage Dynamique crée automatiquement les profils d'usage de la base de données et les politiques de sécurité qui vont du niveau granulaire au niveau requête pour chaque utilisateur et application accédant à la base de données. L'audit détaillé de l'activité de la base de données et le reporting permettent de standardiser la conformité aux réglementations en matière d'audit avec zéro impact sur la performance des bases de données. L'analyse unique de l'activité et les technologies de corrélation assurent la gouvernance en temps réel et la protection, en séparant les risques réels et les attaques des variations inoffensives du comportement utilisateur.

Contrôle et sécurité

Évaluation de la sécurité

L'identification des données sensibles (Sensitive Server and Data Discovery) parcourt d'abord le réseau pour localiser tous les serveurs d'applications Web et de bases de données, puis les données sensibles (numéros de cartes bancaires, numéros de sécurité sociale, etc.) qui existent à l'intérieur de ces systèmes. Même les données cryptées peuvent être identifiées et surveillées.

SecureSphere fournit trois capacités uniques d'évaluation distinctes : identification de données sensibles, évaluation de configuration, et évaluation de comportement. Ensemble, ces capacités fournissent, à ce jour, l'analyse de sécurité et de conformité la plus détaillée de l'industrie. L'information d'évaluation de SecureSphere est présentée dans des rapports facilement compréhensibles, qui évaluent le risque, supportent l'action corrective visée et documentent le statut de conformité.

L'évaluation de configuration génère des requêtes dans la base de données pour la conformité avec plus de 350 tests de sécurité. La procédure de test couvre des domaines clés comprenant les failles connues de sécurité logicielle, la configuration logicielle, les privilèges, les objets externes et la conformité.

L'évaluation de comportement identifie les vulnérabilités qui peuvent seulement être identifiées en contrôlant le comportement utilisateur au cours du temps. Par exemple, les événements de login sont analysés au cours du temps pour détecter l'usage partagé de comptes administrateur système (ou tout compte) par des utilisateurs multiples - une violation claire mise en exergue sur la plupart des infrastructures de sécurité.

Protection de comportement non autorisé - Profilage Dynamique d'Imperva

La technologie du Profilage Dynamique de SecureSphere crée automatiquement et maintient les profils de base vérifiés de chaque activité utilisateur. Le personnel responsable de la conformité et de la sécurité peut comparer les profils utilisateur aux fonctions, obligations réglementaires ou bonnes pratiques. Les profils peuvent ensuite être personnalisés ou immédiatement convertis en politiques que SecureSphere utilise pour détecter un

comportement non autorisé et des variations de conformité au cours du temps.

Une déviance importante d'un profil autorisé génère une alerte et peut être éventuellement bloquée. Considérez par exemple un spécialiste marketing direct qui normalement extrait des données d'une table clients, mais qui soudain accède à la table des cartes bancaires. SecureSphere reconnaît cette déviance du comportement normal, émet une alerte et peut éventuellement bloquer l'accès.

Responsabilisation utilisateur

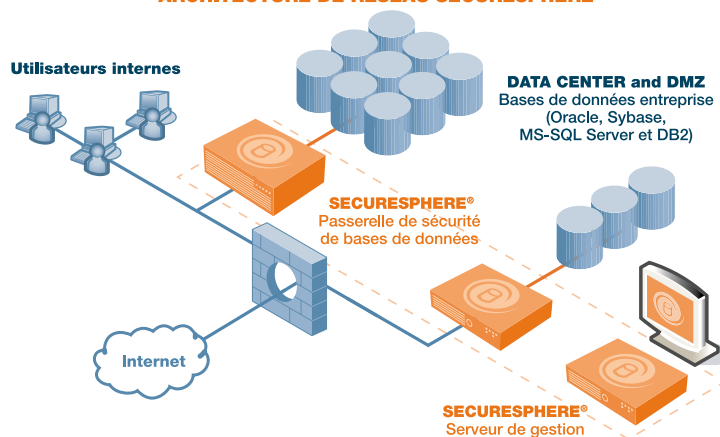
L'un des objectifs principaux de tout système de sécurité consiste en la validation que la responsabilité de l'utilisateur a été établie. Malheureusement, lorsque les utilisateurs ont accès aux enregistrements des bases de données via les applications d'entreprise (Oracle EBS, SAP, PeopleSoft, application propriétaire), les identifiants utilisateur ne sont pas envoyés vers la base de données et ne peuvent donc être détectés par les solutions typiques d'audit, contrôle et sécurité de bases de données.

La technologie de surveillance 'Universal User Tracking' de SecureSphere rend les utilisateurs responsables de leurs actions même lorsqu'ils ont accès aux données via les applications métier. Afin d'identifier les login d'application, une interface dédiée SecureSphere contrôle les sessions utilisateur et les met en corrélation avec les transactions spécifiques des bases de données. Par exemple, un audit SOX avec SecureSphere d'enregistrements financiers relie les identifiants utilisateur aux changements spécifiques dans la base, même si le changement intervient via une application financière.

Protection de plate-forme de base de données

Le système de prévention d'intrusion intégré de SecureSphere (IPS) protège contre les vers et autres attaques visant les vulnérabilités connues des plates-formes de serveurs de bases de données. Les capacités IPS comprennent les dictionnaires de signatures compatibles Snort® (tous protocoles) et signatures propriétaires spécifiques SQL de ADC. De plus, la seule capacité de validation du protocole SQL de l'industrie allège le risque associé au nombre croissant d'exploitations des failles de protocole des bases de données.

ARCHITECTURE DE RÉSEAU SECURESPHERE®



Le pare-feu réseau stateful intégré de SecureSphere protège contre les utilisateurs non autorisés, les protocoles dangereux, les attaques communes de couches réseau et les vers. Les politiques de pare-feu répondent aussi aux exigences de conformité pour réduire l'exposition des bases de données au trafic de réseau non essentiel.

Détection d'attaque sophistiquée

La technologie unique de la validation d'attaque corrélée d'Imperva (Correlated Attack Validation : CAV) met en corrélation les violations au travers des couches de sécurité et au cours du temps pour identifier avec précision les attaques les plus complexes. Certaines violations de profil utilisateur individuel, par exemple, peuvent ne pas indiquer définitivement une attaque. Cependant, en corrélant les combinaisons uniques de profils avec les violations de signatures du même utilisateur, les attaques sont validées au-delà du doute. Aucune autre solution ne peut égaler la précision de SecureSphere via la technologie CAV.

Contrôle local de bases de données

L'agent de contrôle DBA de SecureSphere surveille toute l'activité locale / sur console des bases de données. Le contrôle ne comprend pas seulement l'activité sur console, telnet et ssh, mais aussi s'étend à la mémoire partagée / IPC. Ensemble, les agents et dispositifs SecureSphere garantissent la couverture de l'activité base de données via n'importe quelle méthode d'accès aux bases de données.

Définition de la politique souple d'audit

L'assistant de la politique d'audit de SecureSphere permet le contrôle de tous les événements, ou le pistage sélectif d'un événement sur la base d'une combinaison d'attributs. Les données d'audit vont des attributs de haut niveau tels que les noms utilisateur, à la capture granulaire du texte de requête, texte de réponse, codes de réponse, etc. Aucune autre solution n'égale la capacité de SecureSphere à pister le détail des événements en l'adaptant aux centres de données mondiaux les plus importants.

Efficacité opérationnelle

Politique de sécurité automatisée

La détection de comportement utilisateur non autorisé nécessite la création de profils de base détaillés. Cependant, il n'est pas rentable ou réaliste d'attendre du personnel responsable de l'audit et de la sécurité de créer et maintenir des profils détaillés pour chaque utilisateur, ou même chaque groupe. Les profils peuvent contenir des milliers d'éléments et changent tous les jours.

Le Profilage Dynamique d'Imperva élimine le réglage ou la configuration manuelle des profils utilisateur. SecureSphere applique des algorithmes d'apprentissage adaptatifs pour développer automatiquement et ajuster les profils au fil des modifications de comportement au cours du temps. Cependant, les administrateurs conservent totalement l'accès pour modifier ou créer des profils sur mesure si souhaité. Le résultat final est un investissement de sécurité qui minimise à la fois le risque et le coût total d'acquisition.

Déploiement Transparent – Aucun changement requis

SecureSphere peut être déployé sur le réseau comme passerelle active transparente, routeur en ligne ou moniteur de réseau hors-ligne. Il ne nécessite aucun changement de logiciel des bases de données, du réseau, des serveurs, ou d'infrastructure d'application.

Zéro impact sur la performance, l'administration, ou la disponibilité des bases de données

SecureSphere fournit un contrôle et une sécurité en profondeur sans impacter la performance, l'administration ou la disponibilité des bases de données. Les passerelles SecureSphere ne consomment pas de ressources en bases de données, seul l'agent hôte contrôle l'activité locale - consommant ainsi de faibles ressources. La technologie de l'Inspection Transparente d'Imperva supporte une production multi-gigabits avec une latence inférieure à la milliseconde. De plus, le déploiement de SecureSphere peut être complètement découplé de l'administration des bases de données si souhaité. Enfin, une passerelle avec des options de haute disponibilité assure un temps de service maximum. Les options comprennent la technologie d'Imperva IMPVHA (active/active, active/passive), les interfaces de sécurité, VRRP, STP, RSTP, et le contrôle hors-ligne.

Administration centralisée

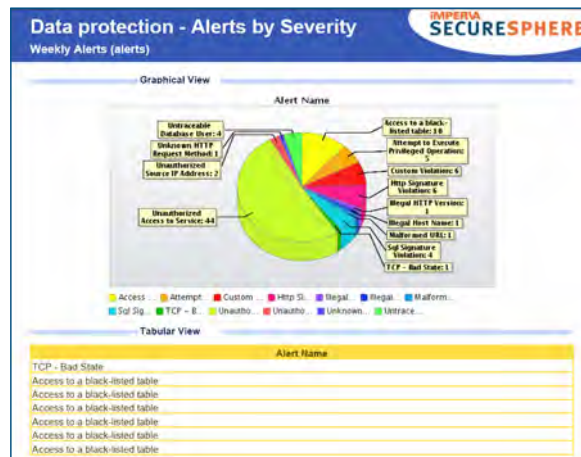
SecureSphere peut être déployé comme dispositif autonome ou distribué au sein de grands centres de données. Pour les environnements importants, le serveur d'administration de SecureSphere (Management Server) offre une configuration, un contrôle et un reporting centralisés. La gestion des grandes entreprises et des environnements ASP est standardisée de façon plus approfondie via des regroupements organisationnels hiérarchiques (clients, unités d'affaires, lieux, etc.), des droits d'accès granulaires basés sur les rôles et un workflow unique orienté tâches d'administration.

Séparation des tâches

SecureSphere présente l'information des bases de données d'une manière accessible aux administrateurs qui ne sont pas ceux des bases de données. En conséquence, SecureSphere peut être géré par le personnel responsable de la sécurité ou de la conformité pour maintenir la séparation des tâches entre la sécurité, l'audit, et l'administration des bases de données si souhaité.

Reporting intelligent

SecureSphere fournit un ensemble "prêt à l'emploi" de rapports de conformité le plus



SecureSphere est capable de sécuriser totalement les bases de données ainsi que l'infrastructure des bases en bloquant activement les attaques malicieuses de bases de données connues.

complet du marché. Il permet d'accélérer l'audit, la sécurité et la conformité vis à vis d'une gamme de cadres réglementaires ou de bonnes pratiques comprenant SOX, HIPAA, PCI, etc. Ces rapports ne se concentrent pas seulement sur les critères

ADC Insight Services – Pertinence de la connaissance

En plus de la passerelle SecureSphere, Imperva offre des services uniques ADC Insight - audit prédéfini, contenu de conformité et sécurité, qui vous maintient à jour avec la connaissance approfondie des plus récentes applications spécifiques telles que SAP et Oracle EBS, des risques liés à ces applications et des réglementations telles que SOX, PCI et HIPAA. Les services ADC Insight fournissent également des modèles basés sur les standards de sécurité industrielle et les bonnes pratiques pour répondre aux exigences d'audit, de conformité et sécurité.

réglementaires spécifiques, mais sur ceux qui sont pertinents pour les applications telles que SAP et Oracle EBS. Aucune autre solution de sécurité de bases de données n'offre la capacité "prêt à l'emploi" de se concentrer sur les questions d'audit concernant les obligations de réglementations et applications métier. En plus des rapports prédéfinis, l'infrastructure de reporting robuste de SecureSphere permet une souplesse complète de création de rapports personnalisés et de modèles pour des situations de reporting uniques. Elle intègre également les outils d'analyse nécessaires pour documenter la conformité en intelligence avec les environnements métier spécifiques.

Étendre SecureSphere aux applications métier pour le Web

SecureSphere peut être étendu à la protection des applications métier pour le Web avec le pare-feu d'applications Web SecureSphere. Les passerelles de bases de données et pare-feu d'applications Web peuvent travailler ensemble pour permettre une protection avancée contre les menaces externes. Par exemple, les violations de bases de données peuvent être corrélées avec les violations Web en temps réel pour vaincre les injections de commande SQL, les falsifications de paramètres et autres attaques Web avec une précision inégalée. Le serveur d'administration de SecureSphere (SecureSphere Management Server) unifie la gestion des déploiements mixtes web et bases de données. Ensemble, ces produits fournissent la seule solution complète de sécurité et d'audit pour les données applicatives métier.

Usage des modèles de Profilage Dynamique des bases de données

Éléments de profil	Description
Objets de base de données	Tous objets de base de données : requêtes, procédures stockées, opérations SQL, tables, objets systèmes
Utilisateurs	Suivi de modifications d'utilisateur final, application et activités d'administration
Activités métiers et transactions normales	Prévient l'utilisation de privilèges légitimes pour des buts illégitimes
Horaires et lieu de travail	Restreint les utilisateurs à des horaires et lieux de travail normaux
Application / Méthode d'accès	Empêche l'utilisation d'accréditations volées ou faisant l'objet d'un abus

Spécifications du dispositif SecureSphere

Spécification	SecureSphere G4	SecureSphere G8	SecureSphere G16 FTL
Production	500 Mbit/sec	1000 Mbit/sec	2000 Mbit/sec
Transactions SQL/Sec	50 000	100 000	200 000
Latence	Sous-milliseconde	Sous-milliseconde	Sous-milliseconde
Interfaces	6 x 10/100/1000 Mbit/s (max 4 interfaces fibre)	6 x 10/100/1000 Mbit/s (max 4 interfaces fibre)	6 x 10/100/1000 Mbit/s (max 4 interfaces fibre)
Types d'interface	Cuivre/Fibre SX/Fibre LX	Cuivre/Fibre SX/Fibre LX	Cuivre/Fibre SX/Fibre LX
Segments de réseau maximum	(2)Passerelle ; (5)Routeur, Non-en ligne	(2)Passerelle ; (5)Routeur, Non-en ligne	(2)Passerelle ; (5)Routeur, Non-en ligne
Unité de rack	1U ; Modèle FTL 2U	1U ; Modèle FTL 2U	2U
Disque dur	250GB SATA Modèle FTL (2) Hot-Swap 250GB SATA	250GB SATA ; Modèle FTL (2) Hot-Swap 250GB SATA	(2) Hot-Swap 250GB SATA
Disque externe	CD-ROM	CD-ROM	CD-ROM
Taille de rack	Rack 19 pouces (483 mm)	Rack 19 pouces (483 mm)	Rack 19 pouces (483 mm)
Poids	11.34 Kg ; Modèle FTL 29.48 Kg	11.34 Kg ; Modèle FTL 29.48 Kg	29.48 Kg
Alimentation	350W ; Modèle FTL (2) Hot-Swap 750W SATA	350W ; Modèle FTL (2) Hot-Swap 750W SATA	(2) Hot-Swap 750W SATA
Puissance AC	100-240V 50-60 FTL	100-240V 50-60 FTL	100-240V 50-60 FTL
Dimensions	430 mm x 648 mm x 42 mm Modèle FTL 430 mm x 705 mm x 87 mm	430 mm x 648 mm x 42 mm Modèle FTL 430 mm x 705 mm x 87 mm	430 mm x 705 mm x 87 mm
Environnement opérationnel	10°C (50°F) à 35°C (95°F)	10°C (50°F) à 35°C (95°F)	10°C (50°F) à 35°C (95°F)
Environnement non-opérationnel	-40°C (-40°F) à 70°C (158°F) humidité relative 90%, sans condensation à 35°C (95°F)	-40°C (-40°F) à 70°C (158°F) humidité relative 90%, sans condensation à 35°C (95°F)	-40°C (-40°F) à 70°C (158°F) humidité relative 90%, sans condensation à 35°C (95°F)
Certifications EMC	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI

Spécification	Serveur de gestion MX
Unité de rack	1U ; Modèle de tolérance à l'erreur : 2U
Interfaces	2 x 10/100/1000 Mbit/s cuivre
Disque dur	250GB SATA ; Modèle de tolérance aux pannes : (2) permutable à chaud 250GB SATA
Lecteur de disque	CD-ROM
Taille de rack	Rack 19 pouces (483 mm)
Poids	11.34 Kg ; Modèle FTL 29.48 Kg
Alimentation	350W SATA ; Modèle de tolérance aux pannes : (2) permutable à chaud 750W SATA
Puissance AC	100-240V 50-60 FTL
Dimensions	430 mm x 648 mm x 42 mm ; Modèle FTL 430 mm x 705 mm x 87 mm
Environnement opérationnel	10°C (50°F) à 35°C (95°F)
Environnement non-opérationnel	-40°C (-40°F) à 70°C (158°F) humidité relative 90%, sans condensation à 35°C (95°F)
Certifications EMC	FCC, CISPR 22, CE, VCCI

Imperva Inc.
Siège social aux États-Unis
950 Tower Lane
Suite 1550
Foster City, CA 94404
Tél : +1-650-345-9000
Tél : +1-650-345-9004

Siège social international
125 Menachem Begin Street
Tel-Aviv 67010
Israël
Tél : +972-3-6840100
Tél : +972-3-6840200

Numéro vert (États-Unis seulement) : +1-866-926-4678
www.imperva.com

© Copyright 2008, Imperva, Inc.

Tous droits réservés. Imperva et SecureSphere sont des marques déposées d'Imperva, Inc. #DS-DSG-0308_FR

