



RSA

The Security Division of EMC

Brief Solution RSA

**Rationaliser les opérations de
sécurité avec les solutions
RSA® Data Loss Prevention et
RSA enVision®**

À qui s'adresse cette solution?

Exigences des acteurs des centres d'opérations de sécurité

La mission d'une équipe des opérations de sécurité – que ce soit au sein d'une grande entreprise avec une équipe et des ressources dédiées ou au sein d'une petite entreprise avec une seule personne assumant plusieurs responsabilités – est de protéger les ressources informationnelles, en supervisant continuellement l'environnement informatique, anticipant et contrant en temps réel les menaces immédiates et les vulnérabilités à long terme et en fournissant des conseils et principes de sécurité aux dirigeants et aux différentes unités métier.

Pour être efficaces, les professionnels des opérations de sécurité doivent s'appuyer sur des outils permettant de convertir une multitude d'événements se produisant en temps réel en informations exploitables. Pour cela, ils doivent disposer d'un processus performant pour gérer les incidents et réduire le risque. Ils ont aussi besoin d'avoir la visibilité nécessaire pour évaluer l'efficacité des politiques, processus et ressources de sécurité et d'avoir des contrôles pour les optimiser.

Le besoin de découverte des informations

Il y a un vrai changement dans l'approche de la sécurité informatique, évoluant de mesures centrées sur la sécurité périmétrique vers des mesures centrées sur la sécurité de l'information. L'approche périmétrique étant devenue inefficace et trop coûteuse en raison du développement exponentiel des données. L'information est aujourd'hui la colonne vertébrale du business et dans une économie incertaine il est plus important que jamais de concentrer les efforts à sécuriser cette information.

Le problème majeur auquel les professionnels de la sécurité sont confrontés réside dans l'écart entre l'utilisation au quotidien par le business des technologies d'information et des politiques de sécurité d'entreprise. Cet écart – et les barrières organisationnelles qui en résultent – rendent particulièrement délicate l'implémentation des mesures de sécurité traditionnelles. Les professionnels des opérations de sécurité se tournent alors de plus en plus vers des solutions de type DLP (Data Loss Prevention ou Prévention de la perte de données) afin d'identifier les informations critiques à travers l'entreprise et des solutions de type SIEM (gestion des informations et événements de sécurité) pour découvrir et contrôler les risques auxquels l'entreprise est confrontée.

Qu'est-ce que la plate-forme RSA enVision?

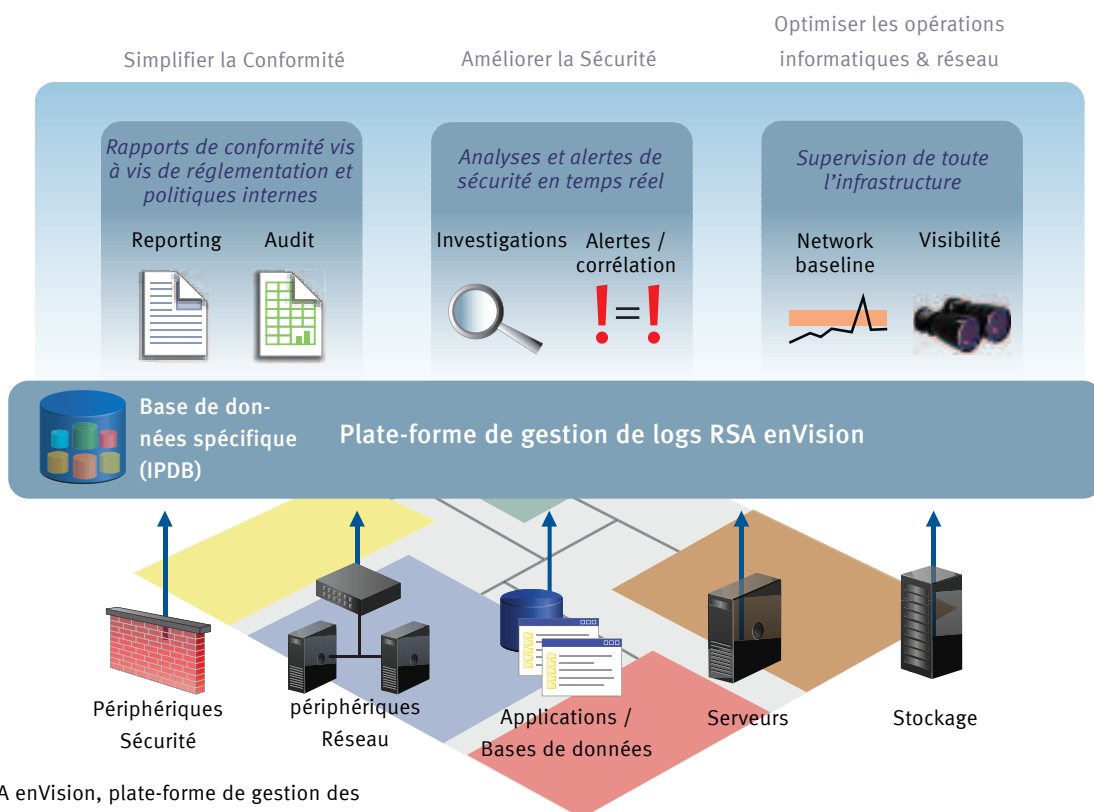
La plate-forme RSA enVision collecte, analyse, corrèle et produit des alertes en se basant sur les données de logs émis par les diverses sources d'événements du réseau et de l'infrastructure informatique. Elle combine également de manière intelligente les données concernant les menaces en temps réel, les vulnérabilités, les ressources informatiques et l'environnement. Ceci aide les organisations à répondre rapidement et complètement aux problèmes de sécurité à haut risque et à localiser les points névralgiques de l'infrastructure. En automatisant les processus manuels et en augmentant la productivité RSA enVision apporte une meilleure sécurité tout en réduisant les coûts.

Avec plus de 1600 clients, de toutes industries, en production dans le monde - dont 5 parmi les 10 du Fortune 10 et 40% des plus grandes banques- la plate-forme RSA enVision :

- fournit des informations de sécurité temps réel, exploitables pour détecter rapidement et précisément les menaces et alerter. Ceci est réalisé en combinant les

données événementielles, les informations sur les ressources et les vulnérabilités. Grâce à des capacités avancées de corrélation, les professionnels de sécurité peuvent prioriser et se focaliser sur les problèmes ayant un impact direct sur l'activité.

- Améliore la productivité des analystes en rationalisant le processus de traitement des incidents. Cette réattribution est possible car enVision offre l'accès aux données réelles empiriques et un workflow intégré qui va de l'identification initiale et la priorisation des incidents, leur investigation avec des données contextuelles, leur escalade, leur résolution, jusqu'à leur clôture et archivage. Les professionnels de sécurité peuvent désormais accélérer concrètement et efficacement la résolution des problèmes. .
- Augmente l'efficacité des mesures et ressources de sécurité en donnant aux équipes de sécurité une visibilité complète sur leur entreprise, l'état des incidents, l'utilisation des ressources de sécurité, et enfin les vulnérabilités et risques pesant sur les actifs critiques. Grâce à des rapports et tableaux de bord complets et intelligibles les équipes de sécurité se focalisent sur les enjeux à haut risque et ajustent leurs politiques, procédures et investissements pour réduire ces risques.



RSA enVision, plate-forme de gestion des informations pour les opérations réseau, sécurité et conformité.

Qu'est-ce que RSA Data Loss Prevention?

RSA Data Loss Prevention (prévention de la perte de données) est une suite intégrée de produits de sécurité des données offrant une approche proactive de la gestion des risques métier liés aux pertes de données sensibles. Ses trois composants (DLP Datacenter, DLP NetWork, et DLP EndPoint) constituent une solution intégrale de prévention de la fuite de données qui:

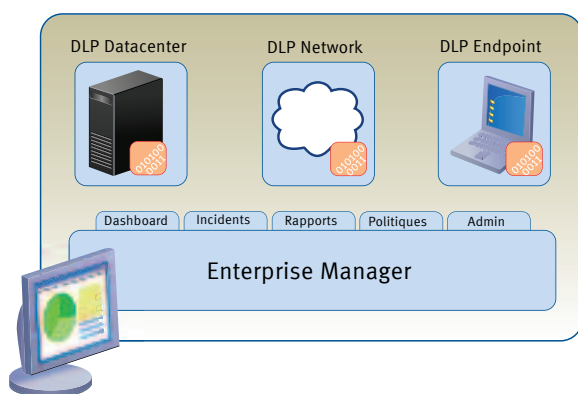
- Découvre et protège les données sensibles dans le datacenter, sur le réseau et sur les postes utilisateurs, tout en mettant en application les politiques à travers l'infrastructure. DLP permet de localiser les données sensibles indépendamment du lieu où elles résident, que ce soit des systèmes de fichiers, des bases de données, des systèmes d'email, des environnements SAN/NAS ou des postes utilisateurs.
- Réduit le risque grâce à une remédiation et une mise en application des contrôles, basées sur les politiques et les identités. RSA DLP exploite les groupes Active Directory sur le réseau et les postes utilisateurs. L'intégration avec Microsoft Rights Management Service® (RMS) apporte des contrôles spécifiques à des groupes et permet une protection au delà des frontières de l'entreprise.
- Réduit le coût total d'exploitation grâce à une évolutivité incomprable, une gestion d'incidents, un workflow des incidents, et une bibliothèque complète de politiques. De plus, des politiques optimisées, des contenus types et des modules de classification, construits par une équipe

de recherche dédiée à la classification et aux politiques, sont proposés prêt à l'emploi dans la solution, ce qui permet d'obtenir les niveaux de précision les plus élevés du marché. Il en résulte une réduction du temps nécessaire pour définir et affiner les politiques et un retour sur investissement global du système DLP. La réduction du coût total d'exploitation est optimale car d'une part on capitalise sur le matériel existant du client et d'autre part le temps de paramétrage initial et de maintenance récurrente est extrêmement limité.

Scenario de déploiement combiné Data Loss Prevention et enVision

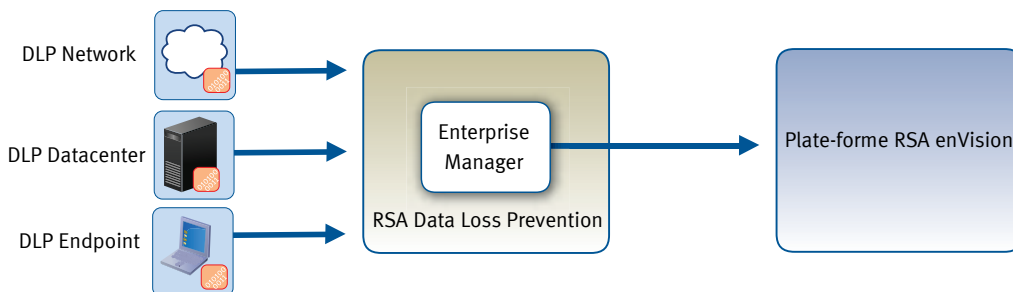
Pour assurer la détection et l'audit initial des données sensibles, le client configure d'abord les politiques et les modules de détection de contenus de RSA DLP. Le module RSA Enterprise Manager reçoit les événements des composants DLP dès qu'une violation de politique est détectée.

A mesure que les événements sont générés, RSA Enterprise Manager les transmet avec les informations utilisateur pertinentes à la plate-forme RSA enVision. Les clients utilisent RSA enVision pour collecter, corréler, analyser et générer des alertes sur ces données d'événements combinées à des ressources et informations utilisateurs d'autres sources. Le retour de cette analyse est à son tour utilisé pour optimiser les politiques de RSA DLP et garantir un stockage et une utilisation appropriés des données.



RSA Data Loss Prevention Suite

La Suite RSA DLP donne une vision intégrale du statut des risques visant les données sensibles de l'entreprise – selon les politiques – indépendamment de l'endroit où se trouvent ces données (dans un datacenter, sur le réseau ou sur des postes utilisateurs).



L'intégration de RSA Data Loss Prevention à RSA enVision offre une combinaison exclusive des fonctionnalités avancées d'analyse, de corrélation et de reporting de la plate-forme enVision aux celles de découverte intelligente des informations de RSA DLP. Cette remarquable complémentarité applique les fonctionnalités de parsing et reporting de logs de RSA enVision à tous les événements DLP, ceux-ci étant transmis par DLP Enterprise Manager à RSA enVision via syslog. À partir de la version 4.0 de RSA enVision et de la version 7.0 de RSA Data Loss Prevention, cette fonctionnalité est automatique, et ne nécessite aucun paramétrage complexe dans l'un ou l'autre des produits. Cette fonctionnalité est proposée à tous les clients existants de la plate-forme RSA enVision à travers leur package mensuel de mise à jour de contenus.

Cas d'utilisation

Cas d'utilisation: Classification de l'impact des incidents de sécurité

Tout professionnel d'un centre des opérations de sécurité (SOC) doit superviser et répondre à de nombreux types d'incidents de sécurité: intrusion de logiciels malveillants, exploitation de failles de sécurité, usurpations d'identité, etc. Grâce à la solution intégrée enVision et DLP, une corrélation efficace des logs d'événements de sécurité et de RSA DLP, permet aux analystes de déterminer rapidement la sévérité et l'impact de tout incident potentiellement urgent. En offrant une vision précise du type et du niveau de sensibilité de l'information impliquée dans l'incident, DLP aide tout analyste d'un SOC à décider quand et comment corriger le problème et à évaluer ses éventuels dommages.

Cas d'utilisation: Watchlisting

Un analyste SOC peut recevoir une alerte d'enVision indiquant une activité utilisateur suspecte, mais qui ne constitue en elle-même une atteinte de sécurité. Dans ce cas, l'analyste pourrait vouloir corréler cette activité suspecte avec les autres activités du même utilisateur. En utilisant la plate-forme RSA enVision avec des données événementielles de RSA DLP, l'analyste peut rapidement collecter toutes les informations sur cet utilisateur et mettre en lumière une structure d'actions, qui prises dans leur ensemble, peuvent représenter un risque de sécurité bien plus sévère que l'alerte d'origine. Par exemple, l'envoi par un utilisateur d'une feuille de calcul financière à une adresse e-mail personnelle peut générer une alerte, mais cette dernière ne deviendra plus sérieuse que si l'analyste s'aperçoit que l'utilisateur en question a également copié différents autres documents sensibles sur sa propre clé USB.

Cas d'utilisation: Investigation des mouvements de données

Alors que l'analyste SOC exploite les événements de RSA DLP pour prendre des décisions en temps réel sur les failles de sécurité, l'analyste «forensic» lui s'appuie sur ces mêmes données pour améliorer l'investigation interne. Incorporer les événements DLP à la plate-forme enVision permet à un analyste de voir au-delà de l'identification des référentiels de données auxquels un utilisateur a accédé. Il peut maintenant voir exactement à quelles données l'utilisateur a eu accès, leur niveau de sensibilité et les actions que l'utilisateur a entrepris ou tenté de réaliser sur ces informations.

Alors que précédemment l'analyste ne pouvait que constater qu'un utilisateur sous investigation, avait eu accès à un site SharePoint® particulier, il peut maintenant prouver que le site Sharepoint contenait une liste sensible de clients que l'utilisateur a copiée ensuite sur une clé USB et aussi adressée par e-mail à un concurrent potentiel - tout ceci au sein de la même interface enVision. Un tel niveau de détails sur l'information, apporte à tout analyste SOC une capacité incomparable pour analyser les incidents de sécurité.

Cas d'utilisation: Découverte de données critiques métier

La découverte de la localisation des données sensibles et leur mode de protection constitue la première étape de sécurisation de ces données. Grâce à la parfaite intégration entre RSA DLP et RSA enVision, toutes les informations sur les ressources de sécurité critiques et les données sensible d'entreprise peuvent être sauvegardées et analysées en un seul endroit. Désormais la plate-forme RSA

enVision devient l'outil centralisé pour contrôler l'état de vulnérabilité des différents actifs du système d'information et pour corréliser ce statut avec les informations métier que ces actifs hébergent.

La création de cet dépôt central d'information présente de nombreux avantages, allant de la simplification du processus de génération de rapports (grâce à une interface unique) à l'amélioration de la boucle de feedback, ce qui permet d'affiner et optimiser avec plus de pertinence les mesures de sécurité existantes. A firewall, for instance, may be modified to be more restrictive once the data that it protects is learned to be extremely sensitive. It is the combination of DLP and the enVision platform that makes this type of holistic analysis feasible. Un pare-feu pourra par exemple être modifié et rendu plus restrictif, s'il apparaît que les données qu'il protège revêtent un caractère particulièrement sensible. C'est la combinaison de DLP et de la plate-forme enVision qui rend ce type d'analyses olistiques faisables.

FONCTIONNALITÉ	BENEFICE
Intégration automatique de RSA Data Loss Prevention au flux d'événements enVision	- Enrichir en temps réel l'environnement SOC avec des métriques de « sensibilité métier »
Rapport des violations de sécurité par utilisateur, département, information et infrastructure	- Découvrir les données sensibles et toutes les informations liées pour permettre l'action sur les processus métier défaillants
Requête sur les incidents utilisateur ou ressource en fonction de la sensibilité des informations	- Prioriser et corriger les incidents de sécurité selon la sensibilité de l'information - Investiguer les mouvements de données y compris, activités d'accès utilisateur, mouvement de données, criticité des ressources & informations.

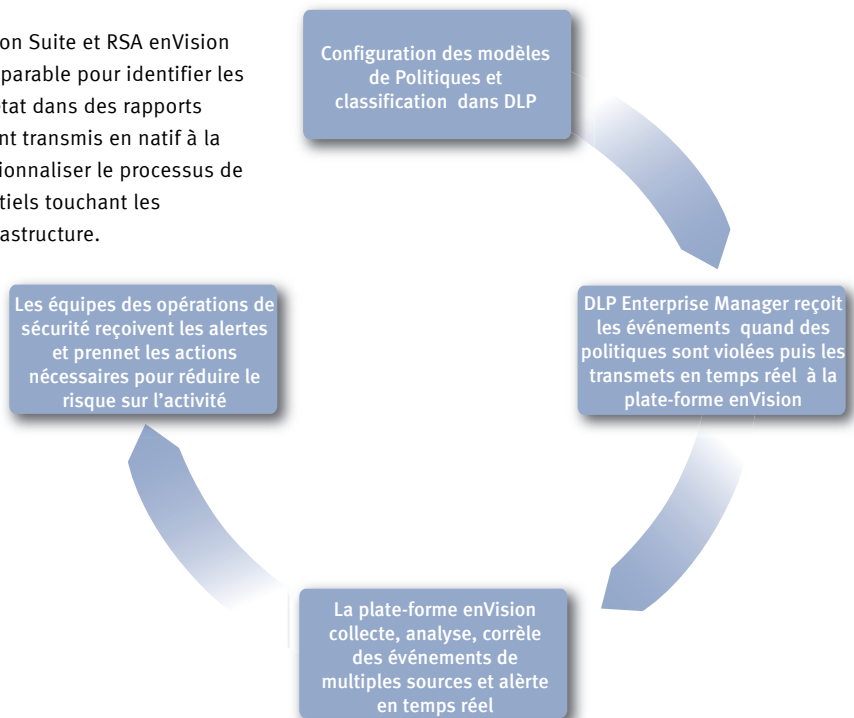
Cas d'utilisation: Supervision des utilisateurs privilégiés

L'information et ses utilisateurs évoluent en permanence faisant du reporting de conformité une quête permanent. Seule, la plate-forme RSA enVision offre l'alerte et le reporting sur l'accès aux données par utilisateur. En rajoutant les événements DLP dans la plate-forme enVision, les spécialistes de la sécurité peuvent proposer un niveau supplémentaire de reporting qui indique non seulement quelles données ont été consultées mais aussi leur niveau de sensibilité ou confidentialité. Les analystes peuvent par conséquent produire des rapports de conformité complets montrant quels types de données sont accessibles aux utilisateurs privilégiés, quelles données ayant été effectivement consultées et quels déplacements de ces données affectent la conformité.

Conclusion

L'intégration de RSA Data Loss Prevention et la plate-forme RSA enVision offre une association exclusive entre les fonctionnalités avancées d'analyse, de corrélation et de reporting de la plate-forme enVision avec celles de découverte des informations de RSA DLP. Ensemble, RSA DLP et RSA enVision constituent une solution complète pour offrir une sécurisation des données centrée sur les impératifs métier. allowing them to fine-tune controls and report on access more effectively than ever before. En complétant les méthodes d'audit traditionnelles par une découverte intelligente de l'information et de la criticité de leur contenu, les entreprises peuvent enfin voir précisément où résident leurs données sensibles et comment celles-ci sont protégées, ce qui rend l'optimisation des mesures de contrôle et le reporting relatifs aux accès, plus efficaces que jamais.

Ensemble, RSA Data Loss Prevention Suite et RSA enVision font preuve d'une efficacité incomparable pour identifier les risques pour l'activité et en faire état dans des rapports complets. Les événements DLP sont transmis en natif à la plate-forme RSA enVision pour rationaliser le processus de compréhension des risques potentiels touchant les informations, les identités et l'infrastructure.





RSA, votre partenaire de confiance

RSA, la Division Sécurité d'EMC, est l'expert de la sécurisation centrée sur l'information protégeant celle-ci tout au long de son cycle de vie. RSA permet aux entreprises de sécuriser leurs ressources informationnelles stratégiques et leurs identités numériques – où qu'elles soient et tout au long de leur cheminement – et de gérer les informations et événements de sécurité pour réduire la complexité de la mise en conformité.

RSA propose des solutions leaders de certification des identités et de contrôle d'accès ; de chiffrement et gestion de clés; de gestion la conformité et des informations de sécurité et de lutte contre la fraude. Cette large gamme de solutions certifie l'identité de millions d'utilisateurs dans le monde, de leurs transactions quotidiennes et des données qu'ils génèrent. Pour plus d'informations, veuillez consulter www.RSA.com et www.EMC.com.

©2010 RSA Security Inc. All Rights Reserved.

RSA, RSA Security, enVision et le logo de RSA sont des marques ou marques déposées de RSA Security Inc. aux États-Unis et/ou dans d'autres pays. SharePoint et Microsoft sont des marques ou marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. EMC est une marque déposée d'EMC Corporation. Tous les autres produits et services mentionnés sont des marques de leurs propriétaires respectifs.

FR DLPENV SB 0409



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC