

Aperçu de la plate-forme RSA enVision™

Une solution de gestion de logs « trois-en-un »

De quoi s'agit-il ?

De nombreux analystes - au nombre desquels le Cabinet Gartner - s'accordent pour reconnaître le leadership de RSA enVision™ sur le marché des solutions de gestion des informations et événements de sécurité (SIEM). RSA enVision™ propose en effet aux entreprises une solution « trois-en-un » unique et intégrée pour : simplifier leurs initiatives de conformité ; maximiser la sécurité et réduire les risques, et enfin, optimiser le fonctionnement opérationnel de leurs réseaux et systèmes d'information. Pour cela, elle automatise les activités de collecte, d'analyse, d'alerte, d'audit, de reporting et de stockage sécurisés de l'ensemble des logs de l'entreprise.

Grandes fonctionnalités

La plate-forme RSA enVision collecte l'ensemble des journaux d'événements générés par tous les périphériques IP du réseau, archive continuellement des copies de ces données, traite les journaux en temps réel et génère des alertes en cas de modèles comportementaux suspects. Les administrateurs peuvent interroger l'intégralité des données stockées à travers un tableau de bord intuitif et des outils analytiques avancés permettant de convertir une grande quantité de données brutes en informations intelligibles et exploitables pour les assister dans trois domaines principaux :

Simplification des initiatives de mise en conformité. La collecte automatisée de l'ensemble des données des journaux (au niveau des réseaux, fichiers, applications et activités des utilisateurs) simplifie le processus de mise en conformité. Intégrant plus de 1100 rapports - spécialement conçus pour répondre aux exigences de conformité actuelles et futures. Cette solution simplifie la conformité avec toute législation apparaissant dans les années à venir, dans la mesure où elle enregistre l'ensemble des données journalisées sans filtrage ni normalisation et les protège contre toute atteinte ultérieure, constituant ainsi une source vérifiable et authentique des données archivées.

Renforcement de la sécurité et réduction des risques. Les fonctionnalités d'alerte de sécurité en temps réel, de supervision et d'investigation par zooms successifs offrent aux administrateurs une vision claire des informations importantes. Grâce à cette visibilité et à une parfaite compréhension des menaces et risques potentiels, ils peuvent mettre en œuvre les actions correctives les plus efficaces pour réduire ces risques.

Optimisation du fonctionnement opérationnel des réseaux et technologies de l'information. L'administration des données journalisées est une source d'information incomparable sur les performances de l'infrastructure et le comportement des utilisateurs. Les équipes de support peuvent ainsi capitaliser sur la plate-forme RSA enVision pour tracer et administrer les journaux d'activité (des serveurs, équipements réseau, plates-formes de stockage, etc.) et également superviser les ressources réseau, la disponibilité et l'état des utilisateurs, matériels et applications métier. RSA enVision fournit un outil avancé d'investigation pour dépanner d'éventuels problèmes d'infrastructure et protéger les ressources de cette infrastructure. Il guide les efforts des responsables informatique dans les opérations de support technique, et propose une visibilité très détaillée des comportements spécifiques des utilisateurs finaux.

Quel est le principe de fonctionnement ?

La plate-forme RSA enVision est capable de récupérer en une seule opération les journaux de dizaines de milliers de périphériques (serveurs Windows®, pare-feux Check Point®, routeurs Cisco®, etc.) sans déploiement d'agent logiciels du côté client. Cette technologie exclusive permet une collecte permanente et continue de toutes les données (« All the Data™ »). Les fonctionnalités de « situation normale » (« baseline »), de tendances et de reporting de RSA enVision permettent aux administrateurs des réseaux et systèmes d'information de construire une vision graphique à long terme des performances et événements de sécurité pour améliorer leur efficacité de planification et réduire la charge de travail. Cette plate-forme peut être déployée en tant que solution autonome, « plug-and-play » ou intégrée à une architecture distribuée, extensible et à haute disponibilité répondant aux exigences des réseaux les plus étendus. Quelle que soit l'option retenue, tous les logiciels nécessaires vous sont fournis - sans supplément de prix.

Grâce à son interface d'administration Web et à sa technologie exclusive d'exploration « RSA enVision Event Explorer™ », le système d'intelligence analytique propose des contrôles particulièrement intuitifs et des analyses détaillées ou post-mortem. Lors d'un déploiement autonome (gamme ES), toutes les opérations de collecte, d'administration, d'analyse et de stockage des données sont réalisées par la même appliance autosuffisante et bénéficiant d'une sécurité renforcée. En architecture distribuée (gamme LS), plusieurs appliances dédiées sont déployées sur le réseau pour accomplir les tâches clés : Des collecteurs locaux et distants exécutent la collecte de données. Les serveurs de données font l'administration des données ; Les serveurs d'applications gèrent l'analyse et le reporting. Les données elles-mêmes peuvent être sauvegardées en liaison directe DAS, en ligne, quasi-en ligne, ou hors ligne, notamment en capitalisant sur le portefeuille de solutions de stockage d'EMC





Quel produit choisir ?

Nos gammes d'appliances ES et LS sont basées sur la même plate-forme matérielle et offrent des conditions de licence répondant à la spécificité de vos exigences métier. Pour choisir le produit le plus approprié, il vous suffit de recenser le nombre d'appareils réseau qui seront supervisés et le nombre d'événements par seconde que vous devrez traiter.

Série ES		ES 560	ES 1060	ES 2560	ES 5060	ES 7560
Description		Appliance SIEM autonome	Appliance SIEM autonome	Appliance SIEM autonome	Appliance SIEM autonome	Appliance SIEM autonome
Événements continus par seconde		500 EPS	1,000 EP	2,500 EP	5,000 EP	7,500 EPS
Nombre maximal de périphériques par appliance		100	200	400	750	1,250
Utilisateurs simultanés de RSA enVision™		6	8	10	12	14
Nombre d'utilisateurs simultanés inclus/maximal d'Event Explorer		1/5	2/5	3/5	4/5	5/5
Stockage		300 GO internes	300 GO internes	300 GO internes	Stockage externe requis	Stockage externe requis
Série LS	LS A60	LS D60	LC L605	LS L610	LS R601	LS R602
Description	Appliance de serveur d'applications	Appliance de serveur de bases de données	Appliance de collecte locale	Appliance de collecte locale	Appliance de collecte distante	Appliance de collecte distante
Événements continus par seconde	S/O	30,000 EPS	5,000 EPS	10,000 EPS	1,000 EPS	2,000 EPS
Nombre maximal de périphériques par appliance	S/O	3,072	1,500	2,048	512	1024
Nombre d'utilisateurs simultanés de la plate-forme RSA enVision™	16	S/O	S/O	S/O	S/O	S/O
Nombre d'utilisateurs simultanés inclus/maximal d'Event Explorer	5/15	S/O	S/O	S/O	S/O	S/O
Stockage	Plate-forme RSA enVision™ NAS 3500					

Spécifications du produit

ENVIRONNEMENT D'EXPLOITATION

Environnement standard Microsoft Windows 2003 Server, à la sécurité renforcée.

Redondance matérielle

ES : mémoire RAM avec protection ECC

LS : 8 Go de RAM avec mise en mémoire tampon complète

ES/LS : alimentations et ventilateurs remplaçables à chaud et redondants

Disques protégés par une configuration RAID-1

GESTION ET SUPERVISION DE L'ENVIRONNEMENT

Gestion hors bande avec IPMI 2.0 ; gestion complète des appliances distantes « headless »

MISE EN RÉSEAU

ES : (2) ports Ethernet 10/100/1000TX inclus, jusqu'à (6) via des interfaces réseau complémentaires

LS : (6) ports Ethernet 10/100/1000TX

OPTIONS DE STOCKAGE

2,75 To de stockage DAS utilisables (reportez-vous à la fiche produit de la plate-forme RSA enVision™ DAS2000)

De 3,5 à 7 To de stockage NAS utilisables (reportez-vous à la fiche produit de la plate-forme RSA enVision™ NAS3500)

NORMES ET REGLEMENTATIONS

Certification ISO 9002, UL1950, CSA22.2 n° 950, EN 60950, FCC Part 15 - Classe A, ICES-003 EN55024 : 1998, EIS5022 : 1998, EN50082-1, VCCI V-3/2000.4, AS/NZS3548

LOGICIELS APPLICATIFS

Plate-forme RSA enVision : base de données RSA enVision LogSmart™ IPDB ; corrélation en ligne et en temps réel, avec notation automatique des menaces ; support périphérique universel ; plus de 1 100 rapports standards avec Assistant intégral ; visualisations et analyses post-mortem avancées avec l'outil Event Explorer ; protection ILM, gestion des politiques de rétention, support du stockage hiérarchisé.

OPTIONS D'ALIMENTATION

Alimentations de 400 W redondantes avec partage de la charge ; commutation automatique 120/240 volts

CARACTÉRISTIQUES PHYSIQUES

74,4 x 44,5 x 8,6 cm (PxLxH) ; glissières de guidage pour montage en rack incluses (nécessite un rack à quatre montants)

Poids: 24,5 kg

GARANTIE

Garantie sur le matériel de 90 jours, pouvant être étendue à cinq ans avec un contrat de maintenance actif.



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

The Security Division of EMC

©2008 RSA Security Inc. Tous droits réservés.

RSA, enVision, All the Data, Event Explorer et le logo de RSA sont des marques ou marques déposées de RSA Security Inc. 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.
31N1 DS 0208