



Fiche produit

## Simplifier la conformité informatique

Plate-forme RSA enVision® – Déployer des programmes de conformité performants, économiques, et basés sur un framework de sécurité

### En bref...

- Visibilité et contrôle globaux et en temps réel pour toute l'entreprise
- Conformité à de multiples réglementations avec un seul système
- Création d'un framework de conformité informatique proactif et personnalisé
- Large gamme de rapports pour répondre à toutes les exigences de conformité

### Conformité multi-réglementations efficace et performante

Partout dans le monde, les entreprises doivent relever d'innombrables défis liés aux nouvelles exigences de conformité – imposées par des gouvernements, groupements industriels, partenaires ou politiques internes – imposant souvent une approche purement réactive, consistant à gérer la conformité au cas par cas, et induisant des implémentations de technologies redondantes et une inflation incontrôlée des coûts informatiques.

Il existe pourtant une solution consistant à s'appuyer sur des standards internationalement reconnus proposant des frameworks de sécurité pour mettre en œuvre une approche plus économique et proactive de la gestion des exigences de

conformité – et, plus généralement, des risques informationnels. En basant les activités de conformité sur ces standards (ISO 27002, ITIL, CoBIT, COSO, etc.), les entreprises peuvent réaliser des progrès considérables pour se conformer simultanément à de multiples exigences (PCI DSS, HIPAA, Sarbanes-Oxley, Directives européennes sur la protection des données, etc.) sans redondance des investissements et sans introduire de conflits entre politiques et contrôles. Ces frameworks permettent également d'optimiser la sécurité générale et l'efficacité opérationnelle en comblant toutes les écarts potentiels de du programme de sécurité de votre entreprise.

### Exigences technologiques sous-jacentes à un framework de conformité

L'une des justifications essentielles de l'adoption d'un framework global de conformité est qu'il offre une bonne visibilité des risques pesant sur les informations sensibles et de la situation de conformité de l'entreprise.

Cette visibilité dépend de contrôles fournissant une information complète et actualisée sur les utilisateurs, ressources, données, processus et politiques actives à travers l'ensemble de l'infrastructure. Un framework ayant pour vocation de simplifier le processus de conformité, il est souhaitable que la collecte et la gestion de ces informations soient aussi transparentes et automatisées que possible.

C'est exactement ce que propose la plate-forme RSA enVision®, conçue spécifiquement pour prendre en charge les principes sous-tendant les grands standards tels qu'ISO 27002 et simplifier les initiatives de conformité grâce à la gestion du risque informationnel pour toute l'entreprise.



The Security Division of EMC

---

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

---

La plate-forme RSA enVision est une solution tout-en-1 de gestion de logs conçue pour simplifier la conformité, maximiser la sécurité et optimiser les opérations réseaux et systèmes d'information grâce à l'automatisation des activités de collecte, d'analyse, d'alerte, d'audit, de reporting et de stockage sécurisé de l'ensemble des logs. La collecte automatisée des logs relatifs aux réseaux, fichiers, applications et activités des utilisateurs, permet de prouver le degré de conformité et d'identifier les domaines non-conformes.

La plate-forme RSA enVision offre de puissantes fonctionnalités essentielles à l'établissement d'un programme à base de framework, à savoir :

- Identification automatisée des ressources, données et activités normales de l'entreprise – essentielle pour évaluer le risque et formuler des plans d'action.
- Collecte, gestion et archivage automatisés et sécurisés des journaux issus de tous les composants de l'infrastructure – même ceux gérés par des tiers – pour optimiser la sécurité globale de l'entreprise.
- Monitoring continu des composants réseau et des systèmes d'information métier pour suivre les activités, incidents et événements de sécurité et offrir les moyens de répondre à toutes les exigences réglementaires en termes de contrôle d'accès et de configuration, de détection des programmes malveillants, d'application des règles de sécurité, de gestion et de surveillance des utilisateurs, et de sécurisation de l'environnement et des transmissions.
- Envoi d'alertes aux administrateurs pour notifier les incidents de sécurité en temps réel et permettre la mise en œuvre rapide d'actions correctives. La gestion des incidents joue un rôle prépondérant dans l'établissement d'une conformité effective.

### Simplification du reporting dans tout l'écosystème de conformité

La plate-forme RSA enVision fournit également une fonctionnalité très avancée de reporting pour simplifier la démonstration de conformité. Pour répondre aux réglementations applicables à votre métier et s'adapter à des frameworks et politiques de conformité spécifiques, les administrateurs peuvent créer leurs propres rapports à l'aide d'assistants ergonomiques. Ils peuvent également partir des

plus de 1.100 modèles de rapports couvrant les principales réglementations internationales (SOX, HIPAA, PCI DSS, FISMA, SAS 70, etc).

Point crucial d'une approche normalisée de la conformité, la plate-forme RSA enVision inclut une suite complète de rapports prêts à l'emploi directement alignés sur les spécification ISO 27002. Ainsi, si vous avez adopté ISO 27002 pour administrer l'ensemble de vos contraintes de conformité plus efficacement, vous disposez déjà de multiples fonctionnalités de reporting prêtes à l'emploi pour répondre à vos besoins. La plate-forme propose plus de 20 rapports intégrés pour ISO 27002, dont :

- Contrôle des données de ressources humaines (8.3)
- Rapport sur les prestataires externes (8.1.3, 10.7.3)
- Activités de logiciels malveillants (10.4.1)
- Modifications et expirations de mots de passe (11.3.1)
- Activités des utilisateurs depuis des domaines externes (11.4.2)
- Activités de connexion aux comptes des postes de travail (11.5.b)
- Etat de chaque compte de poste de travail (11.5.1)
- Rapport de contrôle des changements (11.6)
- Contrôle des logiciels opérationnels (12.4.1)
- Contrôle des données de test système (12.4.2)
- Accès aux codes source (12.4.3)
- Contrôle des preuves collectées (13.2)
- Contrôle des données d'audit système (15.3.2)

L'intelligence fournie par la plate-forme RSA enVision à travers ces rapports permet d'accélérer le processus d'établissement d'un programme simplifié de conformité. Le reporting RSA enVision offre la visibilité requise pour évaluer les ressources initiales et le risque, pour implémenter des contrôles efficaces et pour suivre les progrès à produire au niveau de la conformité.

### Prise en charge directe des spécifications ISO 27002

En plus de ce reporting avancé, la plate-forme RSA enVision propose des fonctionnalités d'inventaire, de définition d'activité de référence, d'analyse de tendance, de monitoring et d'alerte pour faciliter la mise en œuvre des meilleures pratiques dictées par le standard ISO 27002, et ce en fournissant des informations exploitables pour prouver la solidité des vos politiques et contrôles. Le tableau suivant en présente les grandes lignes.

Section	Bonne pratique ISO 27002	Comment la plate-forme RSA enVision peut vous aider...
<b>Section 10</b> Gestion des communications et opérations		
10.1.1	Documentation des procédures opérationnelles	Supervision, collecte et corrélation de journaux d'audit issus de plus de 150 types de sources pour établir une base de référence et documenter les procédures opérationnelles. Maintenance des identifiants utilisateurs, dates et heures des événements clés et tentatives fructueuses ou non d'accès aux ressources clés. Gestion automatisée du cycle de vie pour s'assurer que les journaux de log sont conservés pendant une période appropriée.
10.1.3	Séparation des missions et responsabilités	Isolation des responsabilités permettant d'accéder aux journaux d'événements pour remplir une mission, sans accès direct et privilégié aux systèmes critiques qui génèrent ces journaux.
10.2.2	Supervision des activités tierces	Supervision des systèmes d'information gérés par des tiers pour s'assurer que tous les éléments sont administrés en toute conformité.
10.3.1	Supervision des systèmes, planification de capacité et de performance	Corrélation des événements de multiples composants infrastructurels pour alerter les opérateurs des problèmes potentiels affectant les utilisateurs et permettre aux entreprises de gérer plus efficacement leur capacité système.
10.6.1	Etablissement de contrôles de sécurité réseau	Supervision des composants réseau (commutateurs, pare-feux, systèmes IDS et VPN, etc.), pour alerter immédiatement les équipes compétentes en cas d'événement de sécurité.
10.8.5	Protection des systèmes métier	Supervision des systèmes d'information métier offrant une visibilité sur le respect des politiques de conformité et sécurité et des alertes aux administrateurs en cas de violation.
10.10.2	Supervision de l'usage système	Supervision et corrélation continues des événements survenant sur tous les systèmes de l'infrastructure avec alertes pour notifier les activités non-autorisées aux administrateurs.
10.10.3	Protection des log d'audit	Protection des preuves grâce à de nombreuses options de stockage sous-jacent et sécurisé
10.10.4	Logger l'activité power-user	Collecte et supervision de tous les types de journaux (y compris ceux des administrateurs).
10.10.5	Analyse des erreurs	Collecte des entrée du journal d'erreurs ; alertes automatisées aux opérateurs en cas d'erreur.
<b>Section 12</b> Acquisition, développement et maintenance des SI Utilisation de technologies de cryptage pour prévenir les fuites de données		
12.5.1	Procédures formelles de contrôle du changement	Supervision et reporting du changement pour corrélation avec les processus agréés
<b>Section 13</b> Gestion des incidents de sécurité informationnelle		
13.1.1	Reporting immédiat des événements de de sécurité	Détection des événements potentiels de sécurité et notification en temps réel aux administrateurs.
13.2.2	Supervision et mesure de l'impact des incidents	Supervision et reporting efficaces des types d'incidents effectifs pour quantifier l'impact potentiel des menaces sécuritaires
13.2.3	Conservation des preuves	Constitution d'une base de données exploitable de tous les journaux événementiels (logs) pour accélérer et simplifier la découverte de tous les événements liés à un incident particulier
<b>Section 15</b> Conformité. Comment répondre aux exigences internes et externes de conformité		
15.2.2	Revue de conformité technique	Monitoring continu des événements de l'environnement pour détecter et notifier automatiquement toutes les activités non-conformes.
15.3.2	Protection des outils d'audit des systèmes d'information	Etablissement de robustes contrôles d'accès permettant aux utilisateurs de consulter les informations des journaux (sans accès direct aux logs eux-mêmes).



### À propos de RSA

RSA, la Division Sécurité d'EMC, est le premier fournisseur de solutions de sécurité pour l'accélération métier et le partenaire privilégié des plus grandes entreprises mondiales pour résoudre leurs challenges de sécurité les plus pressants, complexes et sensibles. L'approche de la sécurité centrée sur l'information prônée par RSA garantit son intégrité et sa confidentialité tout au long du cycle de vie – quels que soient ses cheminements, ses consommateurs ou ses modalités d'utilisation.

RSA propose des solutions leaders de certification des identités et de contrôle d'accès ; de prévention des pertes de données et de cryptage ; d'administration de la conformité et des informations de sécurité et de protection contre la fraude. Cette large gamme de solutions certifie l'identité de millions d'utilisateurs dans le monde et des données qu'ils génèrent lors de leurs transactions quotidiennes. Pour plus d'informations, veuillez consulter [www.RSA.com](http://www.RSA.com) et [www.EMC.com](http://www.EMC.com).

### Informations complémentaires

Pour plus d'informations sur l'approche RSA de la conformité basée sur des frameworks, visitez [www.rsa.com/compliance](http://www.rsa.com/compliance), où vous trouverez :

- Un aperçu de cette approche basée sur un framework normalisé
- Une présentation détaillant comment les solutions RSA peuvent vous aider à implémenter un framework parfaitement adapté aux besoins spécifiques de votre entreprise

- Une fiche descriptive du service de support RSA présentant notre processus d'implémentation d'un framework en cinq étapes
- Une fiche produit explorant la large gamme de solutions qui viennent compléter la plate-forme RSA enVision dans l'implémentation d'un framework de conformité



RSA, le logo de RSA et enVision sont des marques ou marques déposées de RSA Security Inc. aux États-Unis et/ou dans d'autres pays. EMC est une marque d'EMC Corporation. Toutes les marques mentionnées sont la propriété de leurs détenteurs respectifs.