IBM Security

IBM

Simplifier la mise en conformité réglementaire

Avec les bons outils, la conformité ne se résume pas à un coût nécessaire et peut devenir un précieux atout

Livre blanc IBM Security

Protection des données : de nouveaux enjeux réglementaires importants

Afin de lutter contre l'utilisation abusive des données, les juridictions internationales ont établi de nouvelles réglementations générales et sectorielles sur la protection des données auxquelles doivent désormais adhérer de nombreuses entreprises. Il est donc plus que jamais important de connaître et comprendre les obligations qui en découlent. Dorénavant gestionnaires de l'information, le rôle des entreprises en possession de données a considérablement changé au cours des dernières années, en particulier aux États-Unis et au sein de l'Union européenne. Et tout manquement à la nouvelle réglementation peut porter un préjudice irréversible à une marque, mais également exposer les entreprises contrevenantes à de lourdes amendes, voire des peines de prison. Bien entendu, il ne suffit pas de suivre le cadre réglementaire à la lettre pour identifier et lutter activement contre la violation de données.
Au-delà des exigences réglementaires, les volumes de données sensibles et personnelles détenus par les entreprises sont plus que jamais compromis par les menaces qui planent sur ces informations. Le cybercrime, qu'il soit perpétré par des initiés ou par des attaquants externes malveillants et expérimentés, a mis en évidence la valeur inhérente de l'information — et les cybercriminels exploitent la moindre faille en capitalisant notamment votre incapacité à identifier et sécuriser correctement les données sensibles. Mais, avant de vous intéresser à la question de la sécurité des données, vous devez d'abord réussir votre mise en conformité réglementaire — et vos audits.

Ce livre blanc examine les quatre règlements principaux, notamment la nouvelle réglementation européenne sur la protection des données personnelles GDPR (General Data Protection Regulation), et montre aux entreprises comment respecter la législation en adoptant les processus et technologies adéquats.

Les données... peuvent être à l'origine de fraudes financières dévastatrices, voire de divulgations embarrassantes.[1]

Découvrez les 10 éléments à prendre en compte lors du choix d'une solution de conformité efficace.

1 Timothy B. Lee, « Here's how phone metadata can reveal your affairs, abortions, and other secrets », The Washington Post, 27 août 2013.

Réussir sa mise en conformité malgré un environnement réglementaire en pleine mutation

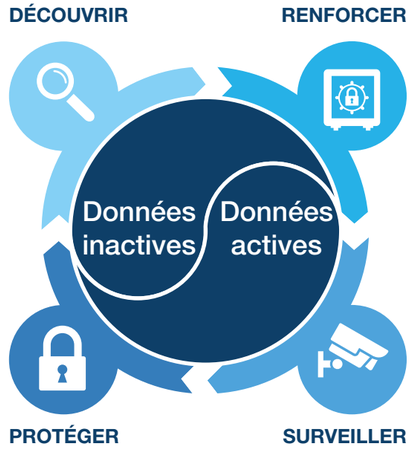
Pendant longtemps, les entreprises se sont conformées aux normes publiées par les gouvernements et organismes internationaux en matière de tenue de registres et de confidentialité pour gérer leurs données — notamment dans les environnements à forte concentration de données et à haut risque. Certains secteurs, comme la santé, les assurances, la gouvernance d'entreprise et les services financiers, sont d'ailleurs très réglementés.

Néanmoins, les nouveaux enjeux réglementaires en matière de protection de données mettent en évidence la valeur croissante de l'information et le profond scepticisme à l'égard des approches mises en œuvre par les entreprises pour respecter la législation. Non seulement les nouvelles réglementations sont extrêmement contraignantes pour les détenteurs de données, mais la jurisprudence a également élargi la définition des organisations et particuliers qui détiennent ou gèrent des données. Les entreprises qui, par le passé, auraient été soumises à des obligations allégées à l'égard des données (sinon aucune) sont aujourd'hui susceptibles de devoir assumer la sécurisation ou la suppression de données qu'elles n'ont jamais créées, ou d'être tenues de supprimer des données qu'elles auraient conservées auparavant.

Pour se conformer aux lois sur le traitement des données, les organisations doivent être capables d'effectuer les actions suivantes :

- **Identifier** et **classifier** les enregistrements sous leur contrôle qui sont soumis à la réglementation
- **Évaluer** et **renforcer** les pratiques et l'infrastructure actuelles afin de respecter les obligations techniques et juridiques
- **Auditer** les processus en interne ou pour les besoins des autorités de régulation, et **rendre compte** des pratiques mises en œuvre en matière de traitement des données (y compris des failles) aux régulateurs et aux sujets de données concernés, aux intervalles fixés ou sur demande
- **Surveiller** les transactions pour l'établissement de pistes d'audit fiables et **mettre en place** des mesures afin d'explorer et d'atténuer les failles éventuelles

Faire de la conformité réglementaire un tremplin vers la sécurité des données



Découvrez comment évaluer et renforcer votre infrastructure de base de données à l'aide de la solution IBM® Security Guardium®.

Loi SOX : responsabilisation, contrôles et divulgation de l'information

Créée au lendemain des différents scandales financiers qui ont fait trembler le pays en raison du manque de transparence des organisations, la loi Sarbanes-Oxley (SOX) de 2002 constitue la plus importante réforme concernant les sociétés qui ont des intérêts avec les États-Unis. La loi SOX est surtout connue pour ses exigences de tenue de registres et de publication qui concernent les grandes entreprises cotées en bourse. Toutefois, elle impose également des règles de gestion qui s'appliquent aux entreprises en tout genre et de toutes tailles. La non-conformité à la loi SOX est passible de sanctions civiles et pénales.

Dans un souci de protéger les actionnaires et le grand public des pratiques comptables frauduleuses et des relations d'initiés non divulguées — mais également d'améliorer la fiabilité des informations et rapports publiés obligatoires —, la loi SOX prévoit notamment la divulgation de certaines décisions et relations en matière de gouvernance d'entreprise. Elle impose également aux entreprises de certifier la validité de leurs états financiers par les dirigeants. Au-delà de la certification, la loi SOX prévoit que les dirigeants et les auditeurs mettent conjointement en place des contrôles internes et rendent compte de leur exactitude.

La loi resserre également la surveillance des conseils d'administration, et applique des sanctions pénales en cas d'interférence avec le travail des auditeurs externes chargés d'examiner les comptes financiers de l'entreprise. Pour se conformer à la loi SOX, les entreprises doivent mettre en place une transparence financière totale, au travers d'une planification et d'une conservation des enregistrements rigoureuses.

Des textes similaires à la loi SOX ont été adoptés dans de nombreuses juridictions dans le monde, notamment en Ontario, au Canada[1], et au Japon[2].

▸ Visionnez cette session technique pour découvrir comment la solution Guardium peut vous aider à relever les défis de la loi SOX.

1 « Keeping the Promise for a Strong Economy Act, 2002, », Assemblée législative de l'Ontario, Canada.
2 « Financial Instruments and Exchange Act », Agence des services financiers japonaise (FSA).

Loi HIPAA : confidentialité des informations de santé

Aux États-Unis, les données médicales des patients doivent respecter les exigences du Titre II de la loi HIPAA (Health Insurance Portability and Accountability Act). Parmi les autres obligations, la loi HIPAA prévoit un traitement confidentiel strict des données médicales protégées (PHI) des citoyens de la part des assurances maladie, des prestataires de services médicaux et autres professionnels de santé. La loi concerne les informations personnellement identifiables (PII) relatives à l'état de santé, aux soins ou au règlement de soins d'un individu. Ses obligations sont interprétées dans une large mesure afin que la loi ne se limite pas au personnel médical et d'assurance seul, mais à une longue liste de fournisseurs[1] disposant d'un accès aux données des patients.

Même s'il est possible d'exploiter les informations des patients à des fins adéquates très spécifiques (pour faciliter un traitement médical, par exemple), d'autres usages demeurent formellement interdits. Toutes les informations personnellement identifiables ne sont pas considérées comme des données médicales protégées, mais la capacité de plus en plus sophistiquée à corréler les données agrégées et les métadonnées pour découvrir des informations personnelles sensibles, ainsi que les lourdes sanctions prévues, démontrent que même les données les plus anodines en apparence doivent être traitées comme s'il s'agissait de données confidentielles sensibles. Au-delà des normes strictes encadrant les données personnelles, la loi HIPAA définit un ensemble évolutif de schémas détaillés dans le but de normaliser la transmission électronique des informations de santé en tout genre entre les organismes concernés.

Les contrevenants à la loi HIPAA sont passibles d'amendes pouvant aller jusqu'à 50 000 de dollars par violation avec un maximum annuel de 1,5 million de dollars.[2]

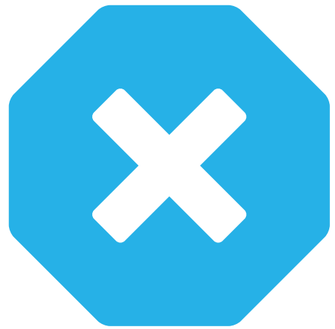
▶ Visionnez cette courte vidéo pour découvrir pourquoi la loi HIPAA et la protection des données de santé et des informations des patients sont plus que jamais importantes.

1 « Emptoris Contract Management for Healthcare HIPAA Compliance », IBM Corp., 2012.
2 « HIPAA Violations and Enforcement », Association médicale américaine.

PCI DSS : protection des données de cartes bancaires et des transactions par carte de crédit

Qu'elles soient réalisées par carte Visa, MasterCard, American Express ou Discover, toutes les transactions par carte de crédit sont soumises à la loi PCI DSS (Payment Card Industry Data Security Standard). Cette réglementation définit un ensemble de mesures et pratiques de sécurité que les commerçants et autres institutions doivent adopter et gérer pour le traitement des cartes de crédit. La norme PCI DSS est une norme propriétaire administrée non seulement par une instance gouvernementale, mais également par un consortium industriel, le PCI SSC (Payment Card Industry Security Standards Council), qui a été créé dans le but d'harmoniser les standards des principaux organismes émetteurs de cartes. Les exigences ou des exigences quasi-équivalentes de la PCI DSS ont, néanmoins, aussi été transposées en lois dans certains états américains. De surcroît, les données concernées par la loi PCI DSS peuvent également être soumises à d'autres réglementations.

Bien que déjà largement répandue, la loi PCI DSS est de nature évolutive. Avec la multiplication des menaces visant l'infrastructure des cartes de crédit et le perfectionnement des outils de lutte associés, elle a été mise à jour à maintes reprises depuis sa création. Par vigilance et pour s'adapter aux évolutions de la norme, les commerçants qui manipulent des données de cartes de crédit sont tenus de faire valider leur conformité tous les ans.



La norme PCI DSS v3.2 a introduit une méthode d'authentification à plusieurs facteurs pour lutter contre les accès non autorisés.[1]

▸ Lisez ce livre blanc pour en savoir plus sur les exigences de conformité de la loi PCI DSS.

1 « PCI DSS 3.2: What's New? » PCI Security Standards Council, 28 avril 2016.

GDPR : garantir la confidentialité des données en plus de leur sécurité

Le nouveau règlement GDPR (General Data Protection Regulation (GDPR), qui remplacera l'actuelle Directive sur la protection des données personnelles, poursuit trois objectifs fondamentaux :
1) créer un cadre juridique unifié en matière de protection des données dans l'ensemble des États membres de l'Union Européenne ;
2) améliorer le niveau de protection des données pour les objets de données européens ;
et 3) moderniser le cadre réglementaire afin de tenir compte des technologies existantes et émergentes. Le règlement a été adopté en 2016 par le Conseil européen et entrera en application le 25 mai 2018.

Le GDPR impose aux entreprises des règles contraignantes dans le but de protéger les données personnelles des citoyens européens, et prévoit des sanctions dissuasives en cas d'infraction. Les principales dispositions sont les suivantes :

- Désignation d'un délégué à la protection des données (DPO) pour les grandes entreprises
- Exercice du « droit à l'oubli » (droit à l'effacement) qui prévoit l'obligation d'effacer les données stockées à caractère personnel
- Mise en place de dispositifs de sécurité efficaces pour protéger les données d'identification personnelle des individus, notamment les informations qui, une fois agrégées, permettent d'identifier personnellement une personne physique

Pour comprendre les enjeux du GDPR, il est important de saisir son impact au-delà de l'Europe. En effet, le nouveau règlement s'applique aux données personnelles appartenant à quiconque vivant sur le territoire européen, que les données soient stockées ou traitées. Par conséquent, toute organisation (y compris celles établies en dehors de l'Europe) qui détient des données sur, ou commercialise des produits ou services à, des individus vivant sur le territoire européen est tenue au GDPR.

Le nombre de résidents européens dont les données personnelles sont soumises au GDPR s'élève approximativement à 510 millions.[1]

Lisez ce guide sur le GDRP, et les 5 conseils pour réussir votre transformation GDPR.

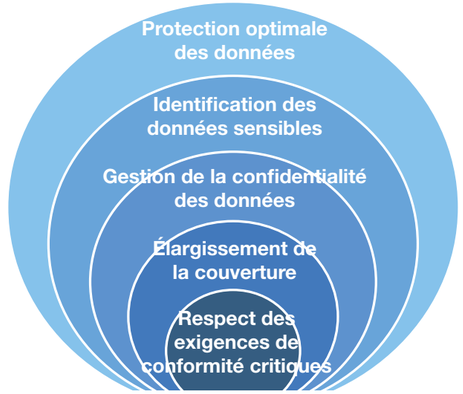
1 « Vivre dans l'UE », Europa.eu.

Planifiez la refonte de votre stratégie de sécurité des données

La refonte de votre stratégie de sécurité est la clé d'une transformation réussie. La mise en conformité est une problématique d'ordre juridique et pratique — une étape cruciale — mais ne constitue qu'un élément d'une équation beaucoup plus vaste. Si la mise en conformité peut certes vous éviter de lourdes sanctions juridiques, cela ne garantit pas que les cybercriminels ne trouveront aucune faille pour pénétrer votre système.

La bonne nouvelle, c'est que les efforts de planification et les plans d'action nécessaires pour réaliser les exigences de conformité peuvent également vous donner un aperçu des objectifs et des outils adéquats pour aboutir à une protection plus optimale des données. On peut comparer la conformité réglementaire à une sorte d'état des lieux propre à un domaine particulier, qui permet de voir à un instant T si les données utilisateur d'une entreprise sont protégées de manière adéquate et si ses enregistrements sont conservés comme il se doit.

Mais, pour respecter les exigences de conformité, les entreprises doivent commencer par examiner l'ensemble des données de fond. Elles doivent notamment s'interroger sur les implications de la sécurité en allant au-delà du cadre des réglementations. Combien de données utilisez-vous activement — et combien avez-vous de données stockées, mais inactives ? Combien de personnes ont accès à ces données, et leur accès est-il contrôlé ? Savez-vous quand quelqu'un accède aux référentiels de données sensibles ? Avec ce genre d'informations, votre équipe sécurité sera à même de mettre en œuvre des recommandations pour protéger vos données et utilisateurs, anticiper les failles potentielles, et planifier activement les plans de défense et d'action en cas de faille.



Pour aboutir à une protection optimale des données, vous devez commencer par répondre à vos obligations réglementaires immédiates, puis identifier et classifier les informations à l'échelle de l'environnement de données.

Découvrez ce que vous devez savoir pour vous préparer à la mise en conformité… et comment en tirer le maximum de valeur en faisant les bons choix !

Pourquoi la conformité est-elle contraignante ?

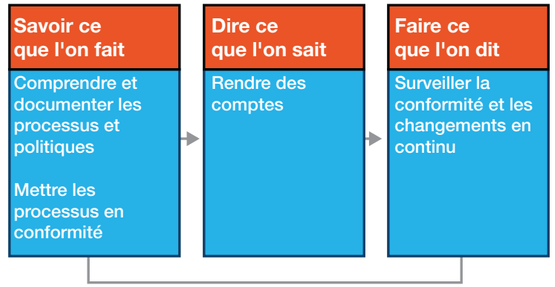
La conformité réglementaire comporte plusieurs dimensions, ce qui peut la rendre contraignante. La stratégie de conformité d'une entreprise doit tenir compte des juridictions qui se chevauchent, mais également de la portabilité des données et de l'évolution des contraintes de confidentialité. Elle ne doit pas se contenter de surveiller l'accès aux données, mais également s'attacher à produire des rapports réguliers sur les activités ainsi que des pistes d'audit réelles. Tous ces facteurs interagissent de manière inévitable. Ils affectent l'approvisionnement en matériel et logiciels, les processus de gestion, les pratiques de sécurité, les politiques du personnel, les relations client, et bien d'autres encore.

Compte tenu du grand nombre de facettes et d'éléments à prendre en compte, les entreprises bloquées en mode réactif — plutôt que proactif — progressent difficilement sur le chemin de la conformité. Il est difficile, mais vital, de dresser un état des lieux de la situation : le type de données que vous détenez, l'endroit où elles sont stockées et la manière dont elles sont utilisées.

À l'heure où les entreprises doivent gérer des données portables, plusieurs sites géographiques et des bases de données client internationales, la situation est devenue plus floue.
C'est pourquoi, avant d'engager votre démarche de conformité, vous devez vous poser les bonnes questions :

- À quel endroit les données concernées par la conformité se trouvent-elles ? Dans vos locaux, dans le cloud ou les deux ?
- Vos données sont-elles utilisées par des applications SaaS (Software-as-a-Service) ?
- À quelles réglementations votre entreprise est-elle soumise ? Votre entreprise est-elle assujettie à des règles spécifiques à un domaine particulier ?
- Quels sont vos besoins en termes de réseau, de flux de données ou d'accès ?

Au fond, toutes les réglementations ont le même but...



La plupart des réglementations s'attachent aux processus, à la gouvernance et à l'obligation de rendre des comptes, mais pas à la technologie.

Lisez ce blogue pour savoir comment dresser un état des lieux de vos données et relever le défi de la conformité.

Les clés pour prendre un bon départ

Toute démarche de conformité nécessite l'élaboration d'un plan solide. Par le passé, les entreprises auraient pu se contenter de repenser les journaux de bases de données et autres approches ad hoc. Or, le besoin en méthodes auditables de traitement de données est aujourd'hui tel que les solutions développées en interne n'en valent pas le risque. Un plan de conformité efficace doit couvrir efficacement plusieurs exigences fondamentales, notamment les suivantes :

- **Recherche et classification des données :** les données concernées peuvent résider dans un nombre insoupçonné de sources de données (bases de données, entrepôts de données, environnements Big Data, fichiers et systèmes de fichiers, environnements cloud, etc.). Vous devez être capable d'identifier et classer l'ensemble de vos données de manière automatique.
- **Surveillance des activités :** vous devez choisir une solution qui sera capable de surveiller les modèles et activités d'accès aux données (lecture, modification ou suppression) afin d'établir une liste des accès et utilisations effectués, et ainsi d'être capable de rendre compte des activités dont ont fait l'objet les données concernées.
- **Création d'une piste d'audit détaillée :** tous les enregistrements créés ne se valent pas. Qu'il s'agisse des données couvertes ou de leur format de stockage/présentation, les exigences liées à la production de rapports varient considérablement d'une réglementation à l'autre.
- **Automatiser la mise en conformité :** la conformité est chronosensible. C'est pourquoi les rapports et les processus de remise doivent être les plus régularisés et automatisés possible.
- **Renforcer les référentiels de données sensibles :** la conformité va plus loin que la classification et la surveillance des données existantes ; la sécurisation des référentiels de données n'est pas une préoccupation ponctuelle, mais doit être envisagée de manière systématique.

L'automatisation de la conformité peut contribuer à l'évaluation et la résolution des vulnérabilités, la surveillance des activités des données, la remise et la validation des rapports, les processus d'escalade et bien plus encore.[1]

Découvrez comment préparer le terrain pour relever les défis de la conformité, et ainsi faciliter la refonte de votre stratégie de sécurité des données.

1 « Compliance Workflow Automation », IBM Knowledge Center.

Engagez une démarche de conformité efficace avec IBM Security Guardium

Plus qu'une solution de sécurité des données complète, Guardium offre de solides fondations en prenant en charge les fonctionnalités clés nécessaires pour rationaliser et automatiser votre démarche de conformité. De l'identification à la classification automatisées des données concernées par la conformité, Guardium vous permet également d'effectuer la surveillance en temps réel de l'activité des données et des fichiers. Ainsi, vous savez et documentez en permanence qui lit et modifie les données tout en créant une piste d'audit détaillée — sans impacter lourdement les performances de vos systèmes. Enfin, la solution vous permet d'effectuer des évaluations de vulnérabilités et de renforcer vos sources de données, empêchant ainsi quiconque d'accéder aux données sensibles par une « porte dérobée ».

Pour accélérer votre mise en conformité, Guardium propose des centaines de rapports personnalisables préintégrés, ainsi que des accélérateurs. Les accélérateurs Guardium, issus des besoins et de l'expérience de milliers d'utilisateurs Guardium, incluent des rapports, des règles et des groupes sur mesure qui simplifient la procédure de conformité réglementaire (PCI DSS, confidentialité des données, SOX, Basel, GDPR, etc.). Les accélérateurs aident votre entreprise à assembler et centraliser rapidement vos données auditables. Guardium automatise également les workflows de conformité en éliminant les tâches manuelles fastidieuses ; le processus de revue et de validation n'a jamais été aussi simple et rapide.

Pour conclure, Guardium aide les entreprises à relever leurs défis de conformité et à s'en servir comme tremplin pour réaliser une sécurisation complète de leurs données.

En déployant la solution Guardium, les entreprises ont enregistré un retour sur investissement de 218 %.[1]

Utilisez notre outil interactif pour évaluer tous les avantages que la solution Guardium peut apporter à votre entreprise.

1 « Étude Total Economic Impact d'IBM Security Guardium », Forrester Research, septembre 2015.

La solution Guardium peut vous aider à viser plus loin que la conformité en mettant en place une stratégie de sécurité complète de vos données

Votre entreprise peut désormais élargir l'utilisation des mêmes fonctions que propose la solution Guardium pour répondre aux besoins de conformité (automatisation de la détection, de la classification et de la surveillance des données sensibles, surveillance de l'accès aux données sensibles envoi d'alertes en cas de comportement anormal) en les appliquant aux données sensibles (y compris les algorithmes propriétaires, les enregistrements RH, les données des partenaires commerciaux, etc.) et en ajoutant la possibilité de protéger les données sensibles actives et inactives grâce à diverses fonctions (blocage, mise en quarantaine, chiffrement, masquage et occultation). Le résultat ? Vous pouvez passer à la vitesse supérieure et enfin mettre en œuvre une protection efficace des données sensibles dans l'ensemble de l'environnement.

Guardium facilite l'analyse des données et des risques en détectant les données sensibles et en découvrant les risques de manière automatique, en protégeant les données actives et inactives, et en s'adaptant à vos nouvelles exigences informatiques (ajout d'utilisateurs, de nouveaux types et volumes de données, ou de nouvelles technologies). En outre, Guardium prend en charge une vaste gamme de sources de données (mainframes, plateformes de Big Data, environnements cloud, fichiers et systèmes de fichiers). La solution propose également des fonctions avancées d'analyse et d'apprentissage automatique ainsi que des outils avancés de détection de menaces, comme la possibilité de rechercher automatiquement des injections SQL et des procédures stockées malveillantes, pour aider les entreprises à identifier de manière proactive et à anéantir rapidement les menaces. La conformité est loin d'être un frein. En capitalisant votre solution et les connaissances acquises, vous pourrez aborder et relever le défi de la conformité aisément tout en engageant une stratégie de sécurité des données efficace.

La solution Guardium permet d'effectuer un contrôle précis des accès au moyen d'une interface très accessible – même aux utilisateurs les moins expérimentés.[1]

▸ Lisez le document Forrester, « Étude Total Economic Impact d'IBM Security Guardium », pour évaluer le retour sur investissement et les avantages qu'un déploiement IBM Security Guardium peut vous apporter — en termes de conformité et de sécurité des données.

1 « Demo: Fine-grained access control with IBM Security Guardium V10 », IBM Corp., 16 octobre 2015.

ETUDES DE CAS : Guardium dans la réalité

De nombreuses entreprises ont choisi la solution Guardium pour piloter leur démarche de conformité dans des environnements très différents. Découvrez comment certains clients IBM ont décidé de relever leurs problématiques de conformité.

Automatiser son processus de production de rapports de conformité

Une mutuelle de santé importante souhaitait surveiller ses bases de données critiques pour détecter les intrusions et les accès commis par des utilisateurs internes privilégiés. Elle voulait également créer une piste d'audit centralisée de ses bases de données au sein d'un environnement hétérogène existant. Le point critique du projet concernait les performances ; la société ne voulait pas de fonctions intégrées aux bases de données, telles que des déclencheurs ou des journaux de transactions, qui risqueraient de compromettre la vitesse et la stabilité de ses bases de données. À importance égale, la société avait également besoin de produire des rapports auditables pour se conformer aux lois SOX et HIPAA. En mettant en œuvre une solution Guardium, la société pouvait automatiser son processus de production de rapports de conformité sans sacrifier les performances de ses bases de données.

Lutter contre les violations commises par des utilisateurs internes

Après avoir constaté des violations de règles par des utilisateurs internes, une multinationale dotée d'un portefeuille de 75 millions de clients a entrepris de nombreuses améliorations afin de piloter efficacement sa conformité SOX et la gouvernance des données. Avec plus d'une centaine de serveurs et encore plus d'instances de bases de données, ainsi qu'un environnement multiplateforme incluant IBM AIX®, HP-UX et Microsoft Windows, le projet promettait d'être ambitieux. C'est pourquoi l'entreprise a adopté une approche progressive en commençant par surveiller les activités des utilisateurs privilégiés, puis en se concentrant sur la confidentialité des données. En optant pour une solution Guardium, la société peut désormais auditer plus d'un million de sessions par jour et produire des rapports automatisés de conformité SOX prêts pour l'approbation.

Guardium prend en charge une vaste gamme de sources de données, comme IBM DB2®, Oracle, Teradata, Sybase ou Microsoft SQL Server, qui s'exécutent sur des plateformes Windows, UNIX, Linux, IBM AS/400, IBM z/OS®, des systèmes de fichiers, des environnements Hadoop et NoSQL, des environnements cloud et bien d'autres encore.[1]

Découvrez comment un client IBM a réussi à engager une démarche optimale de sécurisation des données sensibles grâce à la solution IBM Guardium.

1 « IBM Security Guardium Data Activity Monitor », IBM Corp., février 2016.

Pourquoi IBM ?

De nombreuses entreprises à travers le monde ont choisi les solutions IBM Security pour les aider dans la gestion des identités et des accès, et les accompagner sur le chemin de la conformité au moyen de solutions et d'outils de protection des données. Maintes fois éprouvées, les technologies IBM permettent aux organisations de protéger leurs ressources les plus critiques contre les menaces de sécurité évoluées, mais également de démontrer aux organismes de régulation et d'audit qu'une entreprise a rempli ses obligations de tenue de registres et de protection des données.

À l'heure où de nouvelles menaces et réglementations émergent dans un environnement de données en pleine mutation, IBM peut aider les entreprises à développer une infrastructure de sécurité centrale au travers d'un portefeuille complet de produits, de services et de solutions développées par ses partenaires commerciaux. Par ailleurs, les solutions IBM Security peuvent s'intégrer facilement aux environnements d'autres marques, notamment Oracle, Microsoft et SAP, pour une protection maximale. Les solutions IBM Security sont prises en charge par l'éminente équipe de recherche X-Force qui contribue à la sécurisation des données et infrastructures, sur un vaste choix de matériels (téléphones mobiles, appareils connectés, mainframes).

Fort d'une expertise mondiale, IBM s'est imposé comme le partenaire incontournable au sein de secteurs très réglementés (gouvernements, santé et services financiers). IBM aide les entreprises à réduire les vulnérabilités de sécurité et à gérer les risques dans les environnements informatiques les plus complexes.

IBM exploite l'une des plus vastes organisations de recherche en matière de sécurité, de développement et de livraison dans le monde, surveille plusieurs milliards d'événements de sécurité par jour dans plus de 130 pays et détient plus de 3000 brevets de sécurité.

La solution Guardium peut aider les entreprises de toutes tailles à s'adapter à l'environnement réglementaire changeant, quelles que soient leurs particularités (plateforme, topologie de réseau, types de données).

À propos de Guardium

Guardium offre une solution complète de conformité et de sécurité des données pour aider les entreprises à protéger leurs données sensibles sur l'ensemble de l'environnement. Outre l'analyse des risques, la protection des données sensibles et la gestion de vos nouvelles exigences informatiques (ajout d'utilisateurs, de nouveaux types et volumes de données, ou de nouvelles technologie), Guardium s'intègre totalement aux autres outils IBM Security, tels qu'IBM QRadar®, IBM Security Privileged Identity Manager et bien d'autres encore, pour vous aider à relever vos défis de conformité et sécuriser votre environnement.

Pour en savoir plus

Pour en savoir plus sur les solutions IBM Security, contactez votre revendeur ou votre partenaire commercial IBM, ou rendez-vous sur le site Web : **ibm.com**/security/fr

Pour en savoir plus sur les solutions IBM Security Guardium, consultez le site Web suivant : **ibm.com/software/products/ fr/ibm-security-guardium-family**

En outre, IBM Global Financing propose de nombreuses options de paiement pour financer vos investissements informatiques stratégiques et faire progresser votre activité. De leur acquisition à leur utilisation, nous proposons une gestion complète du cycle de vie des produits et services informatiques. Pour en savoir plus, rendez-vous sur : **ibm.com**/financing/fr-fr

IBM

IBM Security
Route 100
Somers, NY 10589

Produit aux États-Unis d'Amérique
Janvier 2017

WGW03244-FRFR-02