WHITE PAPER

La sécurité dans l'univers du cloud

Les entreprises ont adopté l'informatique en nuage (cloud computing) à un rythme sans précédent, transformant ainsi fondamentalement l'infrastructure informatique des secteurs public et privé. IDC, l'institut spécialisé dans l'étude du marché informatique, prévoit que le chiffre d'affaires des services cloud atteindra 43,2 milliards de dollars américains en 2016, alors qu'il était environ de 18,5 milliards de dollars en 2011. Bien que l'informatique en nuage (cloud computing) dote incontestablement les entreprises d'une remarquable efficacité opérationnelle et leur permet de considérables économies, elle entraîne également des risques et des incertitudes. Les entreprises qui déploient des infrastructures de cloud public, privé ou hybride (la forme la plus courante à l'heure actuelle) se doivent de réduire les risques inhérents de sécurité tout en maintenant la conformité aux réglementations sectorielles et officielles.

Heureusement, les progrès dans le domaine de la gestion de la sécurité et de la conformité des informations ont permis de réduire les risques, d'améliorer les réponses aux menaces, et de réduire considérablement les efforts à développer pour gérer la conformité. NetIQ est un leader de ce domaine. Le présent document présente trois étapes simples pour maintenir la visibilité et le contrôle lors de la phase de migration vers le cloud et explique comment NetIQ peut aider pour chacune d'entre elles.

NetIQ

NetIQ | WHITE PAPER

Table des matières

Avantages de l'informatique en nuage (cloud computing)

L'informatique en nuage (cloud computing) a révolutionné la façon dont les services informatiques fournissent des applications et des services à leurs utilisateurs. Son adoption progresse cinq à onze fois plus rapidement[1] que les logiciels traditionnels, et une portion considérable des budgets informatiques sont de plus en plus orientés vers le cloud.

L'informatique en nuage (cloud computing) apporte aux entreprises de nombreux avantages tangibles, notamment la réduction des charges d'exploitation, une évolutivité accrue et l'amélioration de la réactivité de l'entreprise.

Les défis de la sécurité dans le cloud

En dépit des avantages tangibles de l'informatique en nuage (cloud computing), une migration vers une architecture de cloud public, privé ou hybride présente incontestablement des défis, surtout en termes de sécurité et de conformité. Le service informatique conserve la responsabilité et le devoir d'assurer la sécurité et la conformité, et de gérer les activités de l'entreprise tout en continuant à fournir des services au bon moment, ainsi qu'à l'utilisateur et à l'emplacement opportuns.

Réduction des risques de sécurité

Selon une idée fausse véhiculée sur la migration d'applications et de services vers une infrastructure cloud, cette initiative diminue les risques de sécurité en raison des protections (prétendument) sophistiquées de sécurité réseau offertes par le fournisseur de services cloud. Cette idée est dangereuse, parce que la protection de la confidentialité, de l'intégrité et de la disponibilité de vos données sensibles, et la capacité de démontrer la conformité aux réglementations sectorielles et gouvernementales restent des priorités et, en définitive, continuent de relever de votre responsabilité. Il peut s'avérer catastrophique de se reposer sur les protections qu'offre un fournisseur de services cloud, comme en témoigne la violation de la structure informatique en cloud d'Expedia en 2011 et d'iCloud d'Apple en 2012.

Les fournisseurs de services cloud déploient toujours les pare-feux et systèmes de prévention d'intrusion (IPS) les plus performants pour les défendre contre les cyber-menaces, mais ces périphériques n'atténuent pas les risques associés aux erreurs de configuration du système et aux privilèges administratifs mal alignés (et mal gérés). Ces risques de sécurité s'appliquent tout autant aux systèmes hébergés dans le cloud qu'à ceux présents sur un réseau physique. Il faudrait toujours focaliser son attention sur les systèmes que l'on ne peut pas voir.

Détection des failles de sécurité

Les périphériques IPS, les pare-feux de nouvelle génération (next-generation firewalls, NGFW), et autres systèmes de défense fondés sur les signatures détectent très efficacement les menaces connues. Certains produits peuvent même détecter des menaces inconnues ciblant les vulnérabilités connues du système d'exploitation et des applications. Mais les cyber-menaces les plus sophistiquées et le plus dangereuses à l'heure actuelle incorporent des logiciels malveillants absolument inconnus, conçus spécifiquement pour exploiter les vulnérabilités de type Zero Day dans les systèmes d'exploitation et les applications, dans le cadre d'une menace persistante avancée, ou APT (advanced persistent threat).

[1] « The Top Three Cloud Stocks from Gartner's Magic Quadrant », *The Motley Fool*, le 7 mars 2013.

La surveillance des failles de sécurité des systèmes hébergés dans le cloud peut être beaucoup plus complexe que la surveillance sur un réseau physique. La plupart des fournisseurs de services cloud n'offrent pas aux clients l'accès aux consoles ou aux journaux de gestion de leurs périphériques de sécurité réseau parce qu'ils les utilisent pour surveiller les intrusions affectant de nombreux clients dans un environnement multi-tenants virtualisé. En raison de ce manque de visibilité, il est beaucoup plus difficile, sinon impossible, pour les clients de détecter et de répondre de façon proactive aux menaces qui pèsent sur leurs données sensibles.

Les entreprises telles que le Cloud Security Alliance (CSA) définissent des normes prenant en charge la fédération de la sécurité du cloud et les données d'audit, et garantissent aux clients une meilleure visibilité sur leurs données sensibles. Toutefois, il est trop tôt pour que les fournisseurs commencent à adopter ces normes. Jusqu'à ce que la visibilité des données sensibles hébergées dans le cloud s'améliore, les équipes informatiques doivent catégoriser les types d'informations en cours de création au sein de leur organisation et, en fonction de leur sensibilité et de leur valeur, affecter des niveaux de risque associé. Le service informatique peut alors mieux déterminer les types d'informations adaptés à l'hébergement externe, ainsi que les stratégies et les procédures qui conviennent pour régir l'accès.

Le service informatique peut décider de conserver des informations sensibles en interne, que ce soit dans les applications ou les clouds privés, où il peut empêcher toute violation et tout vol en mettant en oeuvre un contrôle et une surveillance centralisés des personnes y ayant accès.

Conformité aux réglementations

La migration des applications et autres services informatiques vers le cloud ne diminue pas la nécessité de démontrer la conformité aux réglementations sectorielles (comme PCI et NERC) et officielles (notamment HIPAA, FISMA, SOX, GLBA). Toutefois, la démonstration de la conformité aux auditeurs externes peut s'avérer plus difficile dans un environnement cloud car nombre des systèmes de sécurité en place pour sécuriser le cloud sont fournis et contrôlés par le fournisseur de services cloud et non pas votre entreprise.

Les sociétés doivent s'assurer que les données sensibles hébergées dans des services cloud, notamment les clouds privés ou infrastructure IaaS (Infrastructure-as-a-Service), sont protégées et gérées conformément aux stratégies de gestion des données et aux réglementations du secteur. Elles devront également surveiller et valider les niveaux de service et s'assurer que les fournisseurs de services sont constamment en mesure de fournir les niveaux de service et les expériences clients promis.

Trois étapes simples pour plus de visibilité et de contrôle

Les entreprises ne peuvent pas se reposer uniquement sur les systèmes de défense de sécurité de leurs fournisseurs de services cloud externes. Avant de mettre en oeuvre la technologie cloud, les entreprises doivent activement et continuellement activer des contrôles de sécurité rigoureux au sein de leurs systèmes sur site pour être « prêts pour le cloud ».

Un programme de sécurité conçu pour le cloud aide les équipes à gérer la complexité et les risques associés au cloud. En renforçant les contrôles, les systèmes et les stratégies de sécurité au sein de l'entreprise avant d'utiliser les technologies cloud, les équipes peuvent mieux gérer l'inévitable croissance du nombre d'utilisateurs, de périphériques, d'applications et d'échanges d'informations. Un programme de sécurité prêt pour le cloud évoluera au sein d'environnements hybrides composés d'éléments traditionnels et cloud, par exemple les composants de fournisseurs d'IaaS. Les programmes de sécurité prêts pour le cloud sont centrés sur les données et sur la réduction des risques et aident les équipes à respecter les impératifs de sécurité et de conformité sans interruption. Composants d'un programme de sécurité prêt pour le cloud :

- **Surveillance des changements** - les solutions de surveillance des changements contrôlent, identifient et créent des rapports sur les changements inattendus dans les fichiers, plates-formes, applications et systèmes stratégiques, et ce en continue. Ces changements imprévus, et souvent non autorisés, peuvent être accidentels ou malveillants, mais ils compromettent toujours la posture de sécurité et de conformité de l'ensemble de l'entreprise. Par exemple, la surveillance de l'intégrité des fichiers (file integrity monitoring, FIM) est un type spécifique de technologie de surveillance des changements focalisé sur l'intégrité des fichiers clés en comparant leur état actuel par rapport aux bases connues. La FIM alerte le service informatique de la présence éventuelle de code malveillant incorporé au sein des systèmes d'exploitation et applications, dans le but de détecter les menaces qui peuvent avoir contourné les défenses traditionnelles de sécurité.

- **Gestion de la configuration sécurisée** - Les solutions de gestion de la configuration évaluent les paramètres de configuration de sécurité (notamment la conformité des mots de passe, les services activés, les vulnérabilités corrigées et les ports ouverts) des systèmes informatiques stratégiques par rapport aux exigences réglementaires, aux meilleures pratiques en matière de sécurité et aux stratégies des services informatiques de l'entreprise, afin de démontrer la conformité et gérer les risques de sécurité des informations. Si l'une de ces solutions identifie un paramètre de sécurité enfreignant une stratégie de gestion des configurations sécurisée, la solution alerte le service informatique pour qu'il puisse évaluer et, si nécessaire, corriger ce paramètre. Les solutions actuelles de gestion de la configuration permettent aux entreprises, en toute simplicité, de renforcer leurs systèmes informatiques stratégiques et de mettre en oeuvre un solide dispositif de sécurité tout en respectant la conformité.

- **Gestion des comptes privilégiés** - les solutions de gestion des comptes privilégiés permettent au service informatique de contrôler et de vérifier l'utilisation de références pour utilisateurs privilégiés (généralement Active Directory) grâce à la délégation granulaire des autorisations et la surveillance des activités administratives. Ces produits protègent les entreprises contre l'escalade des privilèges non autorisés et permettent d'identifier toute utilisation abusive des comptes privilégiés.

- **Gestion des événements et des informations de sécurité (SIEM)** - Les solutions SIEM procurent une vue globale des systèmes de sécurité informatique d'une entreprise et de ses événements de sécurité connexes. Les plates-formes SIEM agrègent les journaux et autres données liées à la sécurité provenant, entre autres, des pare-feux, plates-formes anti-virus (AV), périphériques IPS, logiciels applicatifs, et mettent ensuite en corrélation ces données disparates, dans un souci de découvrir les menaces cachées.

Ces quatre solutions de sécurité et de gestion des risques fonctionnent ensemble pour aider les entreprises à renforcer la sécurité de leur infrastructure et à réduire les risques. À moins qu'une entreprise exploite ces technologies pour sécuriser en priorité ses systèmes sur site, dans le cadre d'un effort coordonné vouée à devenir prêt pour le cloud, la migration de tout service sur le cloud s'avère plus risquée.

Le processus en trois étapes suivant, intégrant des aspects de surveillance des changements, de gestion de la configuration sécurisée, de gestion de comptes privilégiés, et les technologies SIEM, fournit un cadre solide pour sécuriser les systèmes sur site.

Étape 1 : réduire les risques

La première étape pour la visibilité et le contrôle des systèmes dans le cloud consiste à réduire les risques. Pour cela, vous pouvez réduire la surface d'attaque de votre infrastructure, en surveillant l'intégrité des configurations système et optimisant l'accès des utilisateurs privilégiés.

Réduire votre surface d'attaque. En deux mots, la surface d'attaque d'une infrastructure correspond à l'ensemble des moyens par lesquels un pirate informatique pourrait obtenir un accès non autorisé à un système, effectuer des modifications non autorisées et obtenir des données sensibles. Afin de réduire la surface d'attaque, il faut renforcer les systèmes en configurant l'accès utilisateur uniquement aux applications, services, ports et protocoles jugés nécessaires à l'entreprise. Ensuite, le service informatique doit constamment surveiller et évaluer ces systèmes afin d'assurer qu'ils restent configurés selon les normes des meilleures pratiques.

Il existe une importante variété de logiciels de sécurité pour les services informatiques permettant de gérer, surveiller et mettre en application les pratiques exemplaires de configuration pour les systèmes directement connectés à votre réseau. Dans la phase de planification de la migration vers le cloud, vous devez examiner chacun de ces logiciels afin de déterminer s'ils resteront efficaces dans le cloud, où le fournisseur de services cloud peut ne pas prendre en charge l'accès direct de bas niveau de la même façon que vous le faites dans votre environnement.

Exploiter les structures de sécurité informatique. Pour aider à mettre en application les meilleures pratiques en matière de sécurité informatique et à réduire le risque envers la sécurité du réseau, plusieurs entreprises ont élaboré des structures de sécurité informatique (dont beaucoup sont référencées dans les réglementations de sécurité informatique sectorielles et officielles, notamment PCI et FISMA) comprenant des consignes pour renforcer les configurations de sécurité des pare-feux, routeurs, commutateurs, serveurs, ordinateurs de bureau, ordinateurs portables et périphériques mobiles. Les structures de sécurité informatique les plus courants sont :

- SANS 20 Critical Security Controls
- NIST SP 800-53
- ISO 27001
- COBIT

Les principales solutions de gestion de la configuration sécurisée intègrent des modèles de stratégie pour ces quatre structures. Les utilisateurs peuvent exploiter les tableaux de bord et les rapports qui identifient les hôtes non conformes, et les instructions de correction pour remettre les hôtes en conformité.

Optimiser l'accès privilégié. Lorsqu'il s'agit d'accorder des privilèges pour le personnel informatique, la plupart des experts conviennent que les entreprises devraient suivre le « principe de privilège minimal ». Selon ce principe, les utilisateurs devraient recevoir le plus bas niveau d'autorisation possible et pouvoir quand même faire leur travail. Malheureusement, toutes les plates-formes ne prennent pas en charge les privilèges granulaires requis pour accorder moins de privilèges et, sur de nombreuses plates-formes, la configuration et la gestion de ces privilèges présentent de nombreux défis. Aussi, le principe de privilège minimal ne réduit pas à lui seul les risques que représente un personnel informatique surchargé ou mal intentionné. En exploitant les principales technologies de gestion des comptes privilégiés, installées sur site et sur des plates-formes/services mis en oeuvre dans le cloud, les services informatiques peuvent octroyer des autorisations au personnel informatique via des rôles définis au niveau granulaire, où à chaque rôle est affecté un ou plusieurs droits (autorisations). En outre, pour prévenir une escalade des privilèges utilisateurs, des solutions de gestion de comptes privilégiés plus performantes intègrent une sécurité à double clé, exigeant que deux administrateurs informatiques confirment la demande d'intervention.

Étape 2 : améliorer la réponse aux menaces

Après avoir renforcé les configurations de sécurité sur site et celles des fournisseurs tiers (tels que les fournisseurs IaaS) et optimisé vos comptes d'utilisateurs privilégiés, la deuxième étape pour maintenir la sécurité et la conformité dans le cloud consiste à améliorer votre réponse aux menaces. Pour cela, vous devez détecter les menaces au sein de votre infrastructure hybride, en corrélant ces menaces par rapport aux données d'intelligence générées par vos autres systèmes de défense et en surveillant les utilisateurs privilégiés de manière à identifier d'éventuelles violations d'accès.

Détecter les menaces venant de l'intérieur. Pour détecter les cyber-menaces envers vos hôtes sur le cloud, votre première ligne de défense est constituée par le pare-feu et le système de prévention d'intrusion (IPS) de votre fournisseur de services cloud. Mais les menaces les plus graves ciblent actuellement les vulnérabilités de type Zero Day, vous ne pouvez pas compter uniquement sur les défenses périmétrique de votre fournisseur cloud traditionnel.

Plutôt que de focaliser la protection sur un périmètre qui s'étend maintenant bien au-delà des frontières traditionnelles, les équipes de sécurité doivent cibler les contrôles de sécurité au niveau des données elles-mêmes, où qu'elles se trouvent. Les approches axées sur les données en matière de défense contre les menaces (par exemple le codage et l'utilisation de jetons ou « tokenization » en anglais) sont les méthodes les plus efficaces pour protéger les données critiques et respecter les objectifs de conformité. Les équipes de sécurité doivent étendre l'approche axée sur les données aux systèmes et aux utilisateurs sensibles qui accèdent et interagissent régulièrement avec des données stratégiques. Les solutions de sécurité axées sur les données et focalisées sur les systèmes sensibles sont celles qui surveillent l'activité des utilisateurs privilégiés afin d'identifier tout comportement inhabituel ou accès non autorisé à des fichiers sensibles, ou qui surveillent les événements de sécurité et les modifications en temps réel pour détecter toute modification accidentelle ou malveillante de fichiers et systèmes sensibles.

En adoptant une approche axée sur les données, les équipes de sécurité peuvent détecter plus efficacement et de façon plus proactive les menaces potentielles et atténuer les risques envers les données et les systèmes sensibles. Cette approche permet aux équipes d'atteindre de manière fiable les objectifs de sécurité et de conformité ainsi que les objectifs commerciaux—même si l'environnement informatique devient de plus en plus complexe en raison de l'adoption de technologies perturbantes telles que le cloud.

Intégrer vos défenses de sécurité. L'adoption à l'échelle de l'entreprise de la technologie SIEM s'est fortement développée au cours des dix dernières années. Contrairement aux solutions élémentaires de surveillance qui se bornent à regrouper les journaux, les solutions SIEM intègrent et mettent en corrélation les données d'intelligence de tous vos systèmes de défenses de sécurité, sur site et dans le cloud, et fournissent au service informatique un panneau de commande unique pour répondre aux événements quotidiens de sécurité et identifier des attaques avancées qui auraient pu autrement passer inaperçues. Les principales plates-formes SIEM permettent également une étroite intégration avec les solutions de surveillance des changements pour obtenir des données d'intelligence de sécurité plus riches et accélérer les temps de réponse.

Surveiller les violations des accès privilégiés. Les principaux produits de gestion des utilisateurs privilégiés permettent au service informatique de regrouper des utilisateurs privilégiés dans des rôles, et de consigner l'activité des utilisateurs privilégiés dans une archive sécurisée en lecture seule. Ainsi est mis en oeuvre un suivi d'audit détaillé de toutes les actions des utilisateurs privilégiés, y compris les tentatives d'accès non autorisé aux systèmes, que ce soit sur site ou dans le cloud sur le site d'un fournisseur tiers, tel qu'un fournisseur IaaS, ce qui peut constituer des signes révélateurs de comptes privilégiés compromis lors d'un APT ou autre attaque ciblée.

Étape 3 : réduire les efforts de conformité

La troisième et dernière étape pour obtenir une visibilité et un contrôle de votre infrastructure cloud consiste à réduire les efforts développés pour atteindre et maintenir la conformité aux réglementations sectorielles et officielles, notamment PCI, HIPAA, FISMA, SOX et NERC. Pour atteindre ce résultat, il convient d'adhérer aux structures de sécurité informatique pertinentes, en exploitant la bibliothèque de stratégies au sein de votre solution de gestion de la configuration sécurisée et en automatisant les rapports et les alertes de conformité.

Adhérer aux structures de sécurité informatique. Comme il est mentionné à l'étape 1, de nombreuses réglementations de sécurité informatique sectorielles et officielles font référence aux meilleures pratiques appliquées au sein des structures de sécurité informatique. En tirant parti des solutions best-of-breed de surveillance de l'intégrité des fichiers et de gestion de la configuration sécurisée, à la fois sur vos réseaux physiques et dans le cloud, votre entreprise peut adhérer aux structures pertinentes de sécurité informatique, ce qui réduit les niveaux d'efforts à déployer pour atteindre et maintenir la conformité aux réglementations. Voici des exemples de structures de sécurité informatique et de réglementations de sécurité qui les référencent :

- SANS 20 Critical Security Controls référencé par PCI
- NIST SP 800-53 référencé par FISMA
- COBIT référencé par SOX

Exploiter les modèles de stratégie de gestion de configuration sécurisée. Une stratégie de gestion de configuration sécurisée est constituée de « tests » individuels (et de groupes de tests) décrivant l'état prévue des paramètres de configuration d'un hôte spécifique. Les meilleures offres de produits intègrent des bibliothèques de stratégies, à savoir des ensembles de tests préconfigurés, qui correspondent à toutes les réglementations majeures sectorielles et officielles, y compris celles déjà référencées dans le présent document.

L'assignation de modèles de stratégie réglementaire de gestion de configuration sécurisée à des hôtes internes et basés sur le cloud, affectés par les réglementations de sécurité informatique (notamment les hôtes qui traitent des transactions de cartes de crédit), permet au service informatique de réduire considérablement les efforts développés pour atteindre et conserver la conformité aux réglementations.

Automatiser la création de rapports de conformité. La plupart des informations sur la sécurité des produits, spécifiquement celles ayant des rôles spécifiques dans le processus de mise en conformité aux réglementations, génèrent des rapports standard permettant de démontrer la conformité aux réglementations sectorielles et officielles. Les meilleures solutions de sécurité automatisent la fonction de création de rapports de conformité, ce qui signifie que les rapports de conformité sont automatiquement livrés aux auditeurs internes et au personnel de gestion informatique.

Comment NetIQ peut-il vous aider ?

L'écosystème actuel des cyber-menaces est en évolution constante, ce qui est également le cas des réglementations imposées aux niveaux sectoriels et officiels aux entreprises et organismes fédéraux. Si les outils adéquats ne sont pas mis en place, il peut s'avérer très difficile d'atteindre et de maintenir la sécurité et la conformité dans le cloud (dans les réseaux physiques aussi, d'ailleurs). Heureusement, NetIQ peut vous aider.

Nous avons compris que les approches traditionnelles de réduction des risques en matière de sécurité et de conformité des données ne suffisent plus : vous avez besoin d'une solution exhaustive. Parfaitement compatibles, nos solutions de gestion des identités, de la sécurité et des accès vous aident à contrôler l'accès aux données et services de cloud, à réduire le risque de violations de données dans les environnements hétérogènes et à assurer la conformité avec les réglementations sectorielles et les stratégies de sécurité dans le cloud.

Revoyons les cinq principaux produits NetIQ et découvrons comment chacun d'entre eux contribue aux trois étapes susmentionnées afin d'atteindre et maintenir la sécurité et la conformité de votre entreprise, dans le souci de vous préparer à l'avènement du cloud.

NetIQ® Change Guardian™

NetIQ Change Guardian permet de mettre en oeuvre la surveillance des changements et des activités des utilisateurs privilégiés afin d'aider les professionnels informatiques à détecter et répondre aux menaces potentielles en temps réel. La solution vous avertit des changements au sein de votre environnement distribué, offrant un aperçu détaillé d'Active Directory, ainsi que des fichiers, répertoires, partages de fichiers, clés de registre (sur les hôtes Windows), processus système, etc. Les alertes indiquent également si une action a été autorisée, et comprennent une description détaillée des faits précédant et suivant la modification. NetIQ Change Guardian fournit des informations de sécurité optimisées, comportant les détails nécessaires pour identifier les menaces et enregistrer les modifications, assurant plus de fiabilité et de clarté que les événements de journalisation natifs seuls.

NetIQ Change Guardian permet aux entreprises de sécuriser leurs infrastructures hybrides et de préserver la conformité aux réglementations grâce aux fonctionnalités suivantes :

- **Surveillance des utilisateurs privilégiés**. Établit des journaux sur les activités des utilisateurs privilégiés, notamment les architectes et les administrateurs de réseaux, afin de réduire le risque d'attaques internes.
- **Surveillance des changements en temps réel**. Surveille les modifications apportées aux fichiers, plates-formes, applications et systèmes stratégiques en temps réel pour prévenir les violations et assurer la conformité aux stratégies (inclut la surveillance de l'intégrité des fichiers).
- **Alertes de changement non autorisé**. Fournit des alertes intelligentes dès la détection de changements non autorisés potentiellement liés à un APT ou autre attaque ciblée. Les alertes fournissent les détails nécessaires pour identifier les menaces et enregistrer les modifications, par exemple *qui* a effectué l'action, *quelle* action a été exécutée, *quand* la mesure a été prise, et *où* la mesure a été prise.
- **Création de rapports de conformité**. Crée des rapports automatiquement pour démontrer votre capacité à surveiller l'accès aux données et fichiers stratégiques et satisfaire aux exigences de conformité sectorielles et officielles.

NetIQ Secure Configuration Manager™

NetIQ Secure Configuration Manager permet d'évaluer périodiquement les changements de configuration du système et la création de rapports connexes, et fait correspondre cette configuration aux exigences réglementaires et best practices pour assurer la conformité avec les lois et normes SOX, PCI-DSS, HIPAA/HITECH, FISMA, NERC CIP, et bien d'autres. Ses rapports sur les droits des utilisateurs évaluent les autorisations utilisateurs et fournissent des informations sur les personnes ayant un accès et leur niveau d'accès aux informations stratégiques, ce qui contribue à réduire les menaces.

NetIQ Secure Configuration Manager joue un rôle crucial dans la sécurisation des infrastructures hybrides et démontre la conformité avec les exigences de sécurité informatique grâce aux fonctionnalités suivantes :

- **Évaluation de la configuration**. Propose des modèles de stratégies personnalisables alignés avec des dizaines de structures informatiques et normes réglementaires, et compare en permanence les configurations des systèmes en cours par rapport aux bases reconnues comme correctes. Vous aide à réduire la surface d'attaque du réseau et à démontrer la conformité.
- **Rapports sur les droits des utilisateurs**. Évalue les autorisations d'accès des utilisateurs aux systèmes stratégiques, aide les auditeurs à comprendre qui a accès à quel niveau d'informations stratégiques.

- **Gestion des exceptions de l'entreprise**. Aide à supprimer les alertes de configuration dans les cas où certains systèmes doivent s'écarter des normes approuvées de configuration, dans un contexte autorisé, et documenter les motifs de ces exclusions.
- **Tableaux de bord de sécurité et de conformité**. Via des tableaux de bord personnalisables, communique la posture de sécurité et de conformité des systèmes rapidement et intuitivement, dans le but de répondre aux besoins des diverses parties prenantes.

NetIQ Privileged User Manager

NetIQ Privileged User Manager limite les transactions non autorisées et l'accès à des données sensibles en assurant la gestion des utilisateurs privilégiés et le suivi de tous les environnements Windows, UNIX et Linux. Grâce à cet outil, les administrateurs définissent de façon centralisée les commandes exécutables sur des plates-formes par des utilisateurs privilégiés. Ainsi, seuls les utilisateurs autorisés peuvent réaliser des tâches d'administration spécifiques.

NetIQ Privileged User Manager s'attache à sécuriser les ressources sensibles et à démontrer la conformité aux exigences sectorielles via les fonctionnalités clés suivantes :

- **Gestion simplifiée des stratégies.** Vous permet de créer de manière centralisée des règles de sécurité via une console Web, puis les applique sur tous les systèmes UNIX, Linux et Windows gérés.
- **Gestion proactive des risques.** Enregistre et lit l'activité des utilisateurs, jusqu'au niveau des frappes de touches, avec de puissants outils d'analyse des risques.
- **Conformité continue.** Offre des enregistrements permanents d'audit et le filtrage automatisé des données, dans le souci de prouver la conformité. Ajoute automatiquement les modifications des enregistrements permanents d'audit, et filtre des données pour garantir que les événements à hauts risques soient immédiatement visibles.

NetIQ Directory and Resource Administrator™

NetIQ Directory and Resource Administrator est une solution exhaustive de gestion de comptes privilégiés qui prend en charge les accès à Microsoft Active Directory, ce qui limite les utilisateurs à certaines actions pour bénéficier de vues spécifiques du répertoire global. Il prend également en charge le provisioning utilisateur et autres tâches automatiques tout en aidant à faire respecter les stratégies de sécurité et la séparation des tâches (SoD, Separation of Duties).

NetIQ Directory and Resource Administrator permet de sécuriser les ressources et démontrer la conformité aux réglementations grâce aux fonctionnalités suivantes :

- **Contrôles granulaires des accès**. Vous aide à assigner de manière granulaire des autorisations Active Directory aux utilisateurs informatiques à travers plus de 60 rôles et 300 privilèges.
- **Contrôle de l'escalade de privilèges**. Empêche l'escalade de privilèges non autorisés grâce une sécurité à double clé, exigeant deux administrateurs Active Directory pour confirmer les modifications au niveau des autorisations des utilisateurs.
- **Tâches contrôlées en self-service**. Réduit les coûts en permettant aux utilisateurs de mettre à jour leurs informations personnelles de répertoire et de réinitialiser leurs mots de passe.
- **Journaux et rapports centralisés**. Démontre la conformité aux réglementations via la journalisation centralisée de toutes les mesures administratives et une fonction flexible et exhaustive de création de rapports.

NetIQ Sentinel™

NetIQ Sentinel est une solution exhaustive de gestion des événements et informations de sécurité (SIEM, Security Information and Event Management) qui simplifie le déploiement, la gestion et l'utilisation quotidienne de la technologie SIEM. NetIQ Sentinel s'adapte facilement aux environnements d'entreprise dynamiques et procure les informations véritablement exploitables dont les professionnels de la sécurité ont besoin pour comprendre rapidement la posture de menace et pour hiérarchiser les réponses, à la fois sur site et dans le cloud.

NetIQ Sentinel permet aux analystes de la sécurité de surveiller l'intégrité du système tout en procurant aux auditeurs les rapports complets nécessaires pour pouvoir toujours démontrer la conformité aux réglementations. Principales caractéristiques :

- **Regroupement des informations de sécurité**. Les données de journaux regroupées et autres informations sur la sécurité et le réseau obtenues sur l'ensemble de votre environnement informatique, y compris les pare-feux, systèmes AV, périphériques IPS, passerelles sécurisées Web et de courrier électronique, systèmes de prévention des pertes de données (data-loss prevention, DLP) , applications, bases de données, etc.
- **Détection des anomalies**. Identifie automatiquement les incohérences au sein des environnements physiques, virtuels et cloud de votre entreprise grâce à des règles de corrélation puissantes fournies par les fournisseurs et créées par les clients. Vous permet de créer une ligne de base du trafic réseau « normal » et de détecter les anomalies susceptibles de mettre en évidence des menaces.
- **Exploitation des identités**. Connecte les activités et les événements de sécurité spécifiques aux utilisateurs au sein de l'entreprise grâce à l'intégration avec NetIQ Identity Manager.
- **Rapports de conformité simplifiés**. Automatise les fonctions fastidieuses de création de rapports de conformité pour répondre aux besoins des auditeurs de conformité internes et externes.

Conclusion

L'informatique en nuage (cloud computing) change la façon dont les entreprises et les agences publiques fournissent des services informatiques aux utilisateurs. Toutefois, malgré des réductions de coûts, une évolutivité accrue et l'amélioration de la réactivité de l'entreprise, l'informatique en nuage (cloud computing) peut exacerber les problèmes de sécurisation des systèmes stratégiques et de démonstration de la conformité aux réglementations sectorielles et officielles. L'utilisation croissante du cloud et d'autres technologies facilitant les activités structurelles de l'entreprise peut compliquer votre environnement informatique, qui est déjà suffisamment complexe, en ajoutant des interdépendances et des intégrations sans précédent aux fournisseurs tiers.

Les entreprises peuvent profiter au mieux des avantages d'une infrastructure cloud en mettant en oeuvre en premier lieu le processus en trois étapes décrit ci-dessus au sein de leur propre environnement sur site. Une fois cet objectif atteint, il devient plus simple de déployer les contrôles et les processus adéquats dans le cloud, en fonction des besoins. En suivant ce processus, les entreprises peuvent retrouver la visibilité et le contrôle dont elles ont besoin pour assurer la sécurité de leurs données sensibles dans des environnements hybrides, constitués de systèmes sur site et issus de fournisseurs tiers. Elles peuvent également maintenir la conformité aux réglementations, aspect essentiel pour lequel elles ont tant oeuvré.

Les solutions primées de sécurité et de conformité de NetIQ travaillent entre elles avec votre infrastructure de sécurité informatique existante, pour aider votre entreprise à atteindre et à maintenir ses objectifs de sécurité et de conformité, même dans un environnement cloud.

À propos de NetIQ

NetIQ est un fournisseur international de logiciels d'entreprise qui répond aux besoins en environnements informatiques hybrides en proposant des solutions de gestion des identités et des accès, de gestion de la sécurité et de gestion du datacenter. Grâce à nos solutions, clients et partenaires peuvent saisir les nouvelles opportunités offertes par le paysage informatique complexe et en constante évolution. En alignant les technologies et les méthodes de prestation de services, nos clients sont davantage en mesure de fournir une valeur stratégique aussi rapidement que l'impose le monde dynamique des entreprises.

Pour en savoir plus sur nos solutions logicielles primées, rendez-vous sur www.netiq.com.

Siège mondial
1233 West Loop South, Suite 810
Houston, Texas 77027 États-Unis
International : +713.548.1700
Numéro gratuit pour les États-Unis et le Canada :
888.323.6768
info@netiq.com
www.netiq.com

http://community.netiq.com

Pour obtenir la liste complète de nos bureaux d'Amérique du Nord, d'Europe, du Moyen-Orient, d'Afrique, d'Asie-Pacifique et d'Amérique latine, visitez la page : **www.netiq.com/contacts.**