# Stratégies *pour un* RSSI Efficace

## L'Evolution vers les Nuages

L'informatique dans les nuages et les logiciels fournis sous la forme de services (SaaS) vont clairement continuer de s'imposer et représentent une rupture importante dans le secteur de l'informatique. Ce document explique comment ce nouveau modèle contribuera à améliorer la sécurité et à mieux l'intégrer à l'architecture des services dans les nuages. Parallèlement, cette nouvelle donne permettra aux responsables de la sécurité du système d'information (RSSI) de choisir les meilleurs fournisseurs de prestations dans les nuages et les meilleures applications en mode SaaS pour garantir la sécurité de leurs données et optimiser le fonctionnement et la rentabilité de leurs systèmes tout en se conformant aux exigences de la réglementation.

QUALYS®

# Stratégies *pour un* RSSI Efficace

## L'Evolution vers les Nuages

**SOMMAIRE**



**ANNEXE**



QUALYS®

## PRÉSENTATION

Qui aurait cru, il y a encore à peine quelques années de cela, que les données notamment financières, clients, médicales et marketing, tellement convoitées, passeraient aussi rapidement dans les nuages ? Aujourd'hui, toutes les applications ou presque sont désormais disponibles en tant que service en ligne. Même parmi les partisans de l'informatique dans les nuages, peu d'entre eux pensaient que logiciels et données métier seraient libérés aussi rapidement et, du coup, facilement disponibles en tout lieu, à tout moment et depuis un quelconque équipement. Aujourd'hui, il est plutôt inhabituel que les applications logicielles traditionnelles d'un éditeur ne soient pas complétées, voire remplacées totalement, par une offre SaaS ou dans les nuages.

Nous estimons que la révolution SaaS et de l'informatique dans les nuages peut être bénéfique à l'industrie du logiciel dans son ensemble et à tous ceux dont les activités en dépendent. Par exemple, en tant qu'acteurs de l'industrie, nous savons parfaitement que les logiciels évoluent trop vite pour que l'on puisse suivre le rythme. Les améliorations logicielles, les mises à niveau, les correctifs de sécurité et les nouvelles installations sont un processus sans fin. Peu d'entre nous contesteront le fait que beaucoup trop de vulnérabilités touchent un trop grand nombre d'applications. Au cœur de la tourmente se trouvent les entreprises qui ont dû consacrer d'incroyables ressources pour corriger et atténuer les failles de sécurité.

## LE DÉFI DU LOGICIEL TRADITIONNEL

Selon l'étude « The Laws of Vulnerabilities 2.0 », 59 jours en moyenne sont nécessaires à une entreprise pour corriger ses vulnérabilités. Il y a 5 ans, il lui en fallait 60. Soit 1 jour de moins en 5 ans. Si l'on considère tous les efforts et l'automatisation dont la gestion des correctifs a fait l'objet ces cinq dernières années, il n'y a pas de quoi pavoiser. Au-delà de l'importance même de l'enjeu, cela démontre à quel point l'écosystème actuel des logiciels traditionnels est dépassé.

Rien n'est sans compromis. Mais, parallèlement à tous les avantages du SaaS, il ne fait aucun doute que de nouveaux risques et défis surgiront. Notamment en raison du nombre croissant d'équipements mobiles qui accèdent à des données métier critiques. Et aussi parce que 10% des ordinateurs portables utilisés aujourd'hui risquent d'être perdus ou volés, alors que la plupart ne seront pas chiffrés. Vient aussi se greffer problème de la sécurisation des nouvelles architectures de l'informatique dans les nuages, toutes configurations et tailles confondues.

## UN CATALYSEUR DE CHANGEMENT

Heureusement, les modèles du SaaS et de l'informatique dans les nuages constituent des ruptures positives au niveau de l'infrastructure des réseaux privés et du réseau Internet. Contrairement au déploiement de correctifs propre à chaque entreprise et qui implique nécessairement de répéter le travail pour chaque système et chaque installation, toutes les entreprises bénéficient instantanément des correctifs lorsque les fournisseurs SaaS mettent à jour leurs applications logicielles. Sont ainsi résolus la plupart des problèmes de sécurité — problèmes de correctifs et de configurations logicielles — qui entravent aujourd'hui les systèmes technologiques de l'entreprise. Ainsi, à de nombreux niveaux, ce n'est plus à l'utilisateur mais au fournisseur de services logiciels qu'incombe l'essentiel du maintien de la sécurité d'une application. Le déploiement de correctifs pertinents a une incidence sur tous les systèmes informatiques que les fournisseurs de logiciels SaaS et dans les nuages prennent en charge.

Certains continuent de combattre la migration vers le SaaS et l'informatique dans les nuages, mais cette résistance à l'évolution de l'informatique d'entreprise in situ vers l'informatique dans les nuages ne pourra pas continuer longtemps. Les avantages métier, les économies de coût et la simplification sont trop importants pour que les entreprises les ignorent.

En fait, la plus forte résistance émane aujourd'hui du service informatique et de l'équipe chargée de sa sécurité qui craignent avant tout les conséquences de la perte du contrôle des données au profit d'un fournisseur sous-traitant. Ce raisonnement est mauvais car le marché ne consacrera pas des fournisseurs d'applications dans les nuages ou SaaS qui chercheraient à enfermer les données clients. Au final, c'est le client qui garde toujours le contrôle.

Nous estimons que l'un des défis majeurs du RSSI, que ce soit aujourd'hui ou demain, est d'aider son entreprise à migrer vers les nuages de la manière la plus fiable et efficace possible.

## LE RÔLE ÉMERGENT DU RSSI

En dépit des réserves du département informatique, les entreprises continueront d'adopter le mode SaaS et une informatique dans les nuages. En effet, pour rester compétitives, les entreprises n'auront d'autre choix que celui de simplifier le plus possible l'informatique actuelle. Et le rôle premier et stratégique du RSSI sera de gérer en toute sécurité et avec succès les risques de confidentialité et de sécurité liés aux données évoluant dans les nuages.

Par ailleurs, il est indispensable que les entreprises définissent clairement la manière dont elles peuvent intégrer et sécuriser leur infrastructure actuelle dans la mesure où une part toujours plus importante de cette infrastructure migre vers les services dans les nuages. Les entreprises, les professionnels de la sécurité, les directeurs du système d'information ainsi que les fournisseurs doivent donc travailler ensemble pour que la transformation soit la plus bénéfique possible pour tous. Parmi les structures qui s'investissent sans relâche pour nous permettre dès le départ de bâtir correctement cette nouvelle infrastructure dans les nuages, citons la Cloud Secure Alliance et le Jericho Forum qui promeuvent l'une et l'autre les meilleures pratiques dans le domaine.

Si l'évolution visible vers l'informatique dans les nuages a jusqu'ici consisté à faire migrer des applications et des données vers les nuages, les choses ne vont pas en rester là. En effet, les entreprises externaliseront bientôt non seulement leurs logiciels, mais aussi leur infrastructure réseau. Un jour viendra où l'essentiel de nos activités actuelles sur des réseaux privés — gérer des informations, des applications, des infrastructures et des services — sera accessible instantanément et en toute sécurité partout, depuis un simple navigateur Web. Mieux vaut donc commencer à s'y préparer dès maintenant. Et c'est le RSSI qui sera chargé de piloter la stratégie et de garantir la sécurité informatique, dans l'intérêt de l'activité et le respect de la réglementation.

Le leitmotiv sera l'équilibre.

## ÉQUILIBRE ENTRE SÉCURITÉ ET INNOVATION

Pour réussir, le RSSI aura besoin de nombreuses compétences. Il est évident que l'excellence technique nécessaire à la résolution des problèmes de sécurité tactiques sera toujours majeure, tout comme la capacité à communiquer de manière appropriée avec les techniciens, les responsables de l'entreprise et les membres du Conseil. Cependant, les entreprises devront également prouver qu'elles sont capables d'obtenir des résultats malgré les contraintes budgétaires et avec la perspicacité stratégique nécessaire pour assurer leur développement. En somme, le RSSI devra exceller au niveau de l'innovation, de la technologie, de l'intendance et des performances :

- **Faciliter l'innovation métier**
  Les entreprises envisagent de nouveaux services lucratifs, des investissements stratégiques dans des partenariats ainsi que des opportunités de rachat. Même si l'innovation métier s'appuie sur des technologies telles que la virtualisation, les services informatiques dans les nuages, les équipements mobiles pour les utilisateurs ou les applications basées Web facilement accessibles, les problèmes de sécurité exigeront des stratégies novatrices capables de s'adapter à la croissance de l'entreprise.

- **Mettre à niveau l'infrastructure technique**
  Beaucoup d'entreprises ont reporté leurs investissements dans leur infrastructure technique. Aujourd'hui, les entreprises doivent résoudre des défis infrastructurels tels que la mise à niveau des systèmes d'exploitation sur les points d'extrémité, l'augmentation de la bande passante pour renforcer les performances applicatives et la consolidation des ressources serveurs au sein de centres de données virtuels. Cependant, les priorités en matière de sécurité, dont la protection contre les codes malveillants et le besoin stratégique d'auditer l'infrastructure pour se conformer à la réglementation, doivent être appliquées efficacement et en mettant l'infrastructure à niveau. Le défi du RSSI consiste à faire évoluer les performances de la sécurité pour protéger les applications propriétaires contre les menaces contemporaines.

- **Prendre des initiatives socialement gratifiantes**
  Les entreprises modernes améliorent la qualité de vie grâce à des initiatives telles que la Green IT (informatique verte), qui permet d'économiser l'énergie en utilisant moins de serveurs et de ressources, ainsi que la mobilité dans les nuages et les réseaux sociaux. Le RSSI contribue à l'évolution des normes sociales en s'attaquant aux problèmes de sécurité associés grâce à une panoplie de produits, de services et de formation utilisateurs. Un RSSI responsable sait qu'il ne peut pas s'opposer au progrès en invoquant des raisons de sécurité et cherche des moyens pour aider l'entreprise à participer à des initiatives socialement gratifiantes.

- **Réduire le coût de la sécurité**
  Les équipes chargées de l'informatique et de la sécurité doivent trouver des solutions pour réduire les coûts d'exploitation. Et l'objectif de l'entreprise, qui vise à améliorer en permanence son fonctionnement, conduit le RSSI à rechercher des solutions automatisées qui exigent moins de gestion, des produits moins envahissants qui réduisent les coûts de support ainsi que des stratégies qui facilitent l'innovation métier, modernisent l'infrastructure technique et pilotent des initiatives socialement gratifiantes. Cet équilibre entre initiatives stratégiques, solutions tactiques et dynamique de l'activité est schématisé dans l'illustration 1 ci-dessous.

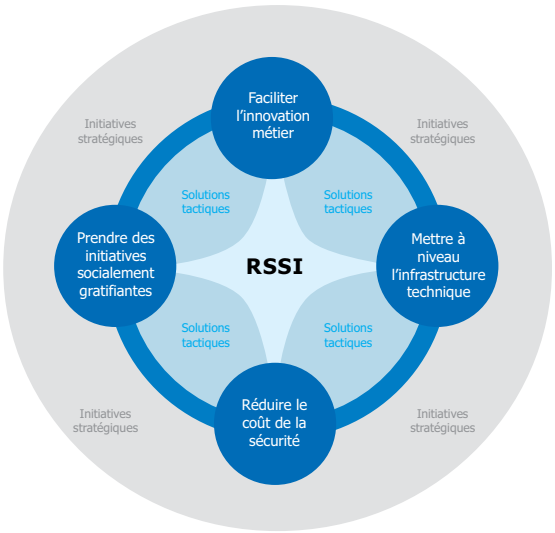



**Illustration 1.** Parvenir à un équilibre entre initiatives stratégiques, solutions tactiques et dynamique de l'activité.

C'est pourquoi un RSSI efficace doit rechercher une stratégie de sécurité pour orchestrer le lancement de nouvelles initiatives métier, piloter l'infrastructure technique et orienter l'entreprise vers des activités socialement gratifiantes. Parvenir à un équilibre entre ces trois objectifs métier relève certainement du défi. En effet, le RSSI peut réduire le coût de la sécurité en achetant moins de produits, mais il laisse alors des failles de sécurité s'introduire dans l'entreprise. Il peut refuser de fournir une stratégie de sécurité aux équipements portatifs et prendre le risque d'aliéner des utilisateurs. Le RSSI peut aussi investir uniquement dans une priorité métier aux dépens des autres. Par conséquent, pour réussir à ce niveau, il est nécessaire de mettre en place une stratégie de sécurité capable d'équilibrer les facteurs métier, les initiatives stratégiques et les solutions tactiques.

Fort heureusement, le modèle de fourniture SaaS permet au RSSI de réussir dans chacun de ces registres. C'est pourquoi les RSSI qui réussissent sont ceux qui adoptent de plus en plus le SaaS comme moyen efficace de sécuriser l'entreprise tout en équilibrant l'innovation, la sécurité et les coûts. Pour toutes ces raisons, le SaaS est un élément stratégique de plus en plus important au sein des arsenaux informatique et de la sécurité. IDC estime que le chiffre d'affaires total des services informatiques dans les nuages passera de 17,4 milliards de dollars en 2009 à 44,2 milliards de dollars d'ici à 2013. Qualys est au cœur de cette évolution stratégique vers les nuages en fournissant des solutions de gestion de la conformité et des vulnérabilités sous la forme de services de sécurité.

## FAIRE MIGRER LES INVESTISSEMENTS VERS L'INFORMATIQUE DANS LES NUAGES

Cette tendance aux applications dans les nuages et SaaS est nourrie par la nécessité pour les grands comptes et les PME d'innover, de simplifier et de réduire les coûts. Grâce à l'approche à la demande de Qualys en matière de gestion de la sécurité informatique et de la conformité, des entreprises de toute taille peuvent gérer les vulnérabilités, la conformité aux politiques et la sécurité des applications Web de manière cohérente tout en réduisant leurs coûts et en rationalisant leur fonctionnement. L'une des principales caractéristiques de la sécurité dans les nuages est l'absence d'équipements ou de logiciels à déployer à travers l'entreprise car c'est le fournisseur SaaS qui héberge ces ressources au sein de centres de données sécurisés. Il y a donc moins d'équipements à déployer et de logiciels à installer pour profiter des mêmes avantages. Outre l'absence de besoins d'équipements, l'économie de l'informatique dans les nuages est régie par des coûts variables décidés par le client en fonction de l'utilisation qu'il fait du service, comme l'explique l'illustration 2.

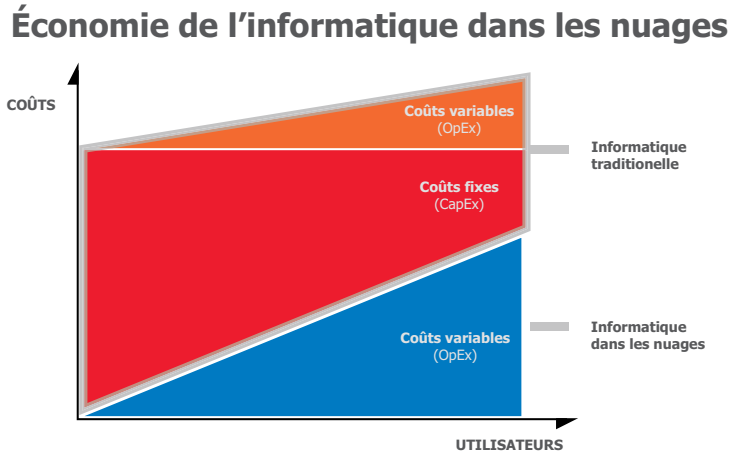



**Illustration 2.** L'économie de l'informatique dans les nuages offre un contrôle total au RSSI

QUALYS®

Influencer le comportement d'autrui a toujours été une compétence clé pour la sécurité, mais l'ampleur des contraintes émergentes est bien plus grande et exige une maîtrise de la psychologie et du marketing ainsi que des compétences en relations sociales. Cette influence nécessite des compétences politiques pour présenter, en personne, un dossier complexe à un comité d'approbation des investissements de même que des compétences en marketing pour mener un programme sophistiqué de sensibilisation à la sécurité et de changement des comportements auprès d'une large base de clients à distance.

Autre compétence essentielle, la capacité à réagir de manière stratégique à un incident majeur mettant en jeu de nombreux partenaires commerciaux et fournisseurs. Outre les atteintes de plus en plus importantes aux actifs intellectuels tels que la réputation de l'entreprise, la complexité croissante des systèmes d'information exige une réponse métier ciblée et élaborée, et non pas un simple ajustement opérationnel. Une réaction stratégique exige des compétences exceptionnelles en coordination de crise ainsi que la faculté de raisonner de manière objective, d'improviser de manière créative et de s'appuyer sur des sources d'information, des services d'investigation et une investigation numérique. Une telle association de compétences est difficile à trouver, à enseigner et à appliquer.

## TROIS AVANTAGES MAJEURS DES APPLICATIONS SAAS

- **Déploiement avec un minimum d'infrastructure ou de ressources humaines**
  Puisque peu voire aucun équipement n'est nécessaire sur site, les équipes chargées de la sécurité peuvent déployer le service dans les nuages à travers l'entreprise avec une relative aisance. L'offre SaaS fournit une solution stratégique qui concerne les nouvelles initiatives métier ainsi que la modernisation de l'infrastructure technique et le support de nouveaux moyens socialement gratifiants pour gérer l'activité de l'entreprise.

- **Exécution uniquement en cas de besoin**
  L'informatique dans les nuages peut être opérationnelle en quelques minutes ou heures et l'utilisation du Web comme mécanisme de transport vers les centres de données du fournisseur augmente réellement la disponibilité du service pour l'entreprise. En outre, chaque fois que l'entreprise sollicite du service, le fournisseur lui envoie automatiquement les dernières mises à niveau fonctionnelles et améliorations du service.

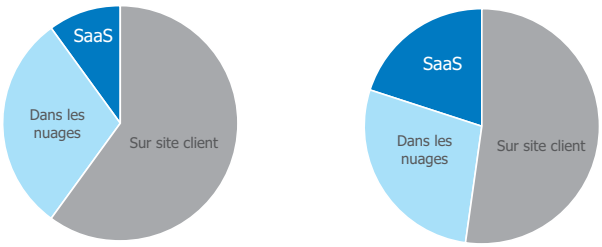
- **Contrôle total des coûts par le RSSI**
  L'application dans les nuages ne s'exécute que lorsqu'elle est demandée, ce qui permet à l'équipe chargée de la sécurité de maîtriser parfaitement les coûts d'exploitation. Évalués sur leur capacité à réduire l'impact de la sécurité sur le chiffre d'affaires, les RSSI font migrer les ressources vers les nuages car aucun investissement en amont en équipements, logiciels et personnel n'est requis et les dépenses sont fonction de l'utilisation qui est faite du service.

## SERVICES DE SÉCURITÉ DANS LES NUAGES POUR GÉRER LES VULNÉRABILITÉS ET LA CONFORMITÉ DE LA SÉCURITÉ INFORMATIQUE

La migration vers des solutions SaaS basées dans les nuages et matures pour assurer la sécurité est devenue trop incontournable pour ne pas emboîter le pas. Voici les principaux enseignements d'Infonetics Research :

les revenus SaaS devraient passer de 10% de l'ensemble des revenus des services de sécurité en 2009 à 22% en 2014, avec un équilibre entre les services de sécurité dans les nuages et sur site client (CPE). En outre, toujours selon Infonetics Research, les revenus mondiaux liés aux services de sécurité fournis en mode SaaS ont augmenté de 70% l'année dernière. Le principal moteur de cette évolution sont les performances élevées des services de sécurité dans les nuages fournis au RSSI pour contribuer à la réussite de l'entreprise.

**art des revenus des services de sécurité SaaS**
**Augmentation sensible de 2010 à 2014**




**Revenus des services de sécurités dans le monde**

© Infonetics Research, "Managed Security Services and SaaS Biannual Market Size and Forecasts", mars 2010.

Outre la facilité de déploiement, la disponibilité permanente et le contrôle des coûts variables offerts par le mode SaaS, la sécurité dans les nuages procure des avantages directement liés à la fourniture de services de sécurité de pointe basés sur l'inspection du contenu ou des systèmes afin de contrecarrer les menaces sophistiquées. Les raisons qui expliquent pourquoi les RSSI efficaces consacrent davantage de leur budget aux services dans les nuages sont faciles à comprendre :

- **Exploitation des toutes dernières informations disponibles sur les menaces.**
  Identifier les vulnérabilités les plus récentes, les codes malveillants ou un site Web non conforme nécessite une équipe de chercheurs dédiée pour identifier la menace et actualiser le processus d'inspection de la sécurité. Une offre de sécurité en mode SaaS, notamment celle fournie par Qualys, épargne au RSSI la distribution coûteuse de mises à jour sur les équipements sur site. L'approche dans les nuages fournit les informations les plus récentes chaque fois que l'entreprise sollicite du service.

- **Automatisation de la vérification de la conformité.**
  Les solutions de sécurité dans les nuages peuvent corréler les informations collectées lors de l'inspection des systèmes pour générer automatiquement des rapports sur les performances de la sécurité et confronter ces résultats avec les exigences de conformité. En automatisant la vérification de la conformité, le RSSI gagne un temps et une énergie précieux tout en permettant aux équipes chargées de la sécurité de superviser en permanence les incidents de sécurité pouvant se produire sur les systèmes critiques.

- **Accès à toute l'entreprise.**
  Avec une solution de sécurité SaaS fournie dans les nuages, le RSSI n'est pas contraint de consacrer toujours plus de temps et de ressources pour distribuer la solution aux centres de données, aux campus et aux équipements distants. L'entreprise distribuée reçoit les mises à niveau directement du fournisseur de sécurité sans qu'il soit nécessaire de les planifier et de les pousser dans toute l'entreprise.

## SOLUTIONS QUALYS DE GESTION DES RISQUES DE SÉCURITÉ INFORMATIQUE ET DE LA CONFORMITÉ À LA DEMANDE

Reconnu comme le principal fournisseur de solutions à la demande pour la gestion des risques de sécurité informatique et de la conformité, Qualys permet aux entreprises de toute taille de garantir facilement, et à moindre coût, la sécurité élevée et la conformité à la réglementation de leurs systèmes technologiques métier. Grâce aux solutions Qualys de gestion des risques de la sécurité et de conformité à la demande, les entreprises sont en mesure de renforcer la sécurité de leurs réseaux et de leurs applications Web. Elles peuvent également réaliser des audits de sécurité automatisés pour garantir la conformité à la réglementation et l'application des politiques de sécurité internes.

Sur le marché de la sécurité, Qualys est le seul fournisseur à proposer ces solutions via QualysGuard®, une plate-forme unique de logiciels fournis sous la forme de services (SaaS). Déployables en quelques heures seulement partout dans le monde, toutes les solutions Qualys à la demande fournissent une vue immédiate de l'état de la sécurité et de la conformité des entreprises utilisatrices. QualysGuard est la solution de sécurité à la demande la plus déployée à travers le monde avec plus de 500 millions d'audits IP par an.

## SÉCURITÉ ET CONFORMITÉ PERFORMANTES

Grâce aux services de sécurité et de conformité fournis par Qualys, les RSSI peuvent à la fois assurer la sécurité du réseau et la conformité aux politiques de manière cohérente, le tout en réduisant les coûts et en rationalisant leur fonctionnement. QualysGuard Security and Compliance Suite comprend le service de gestion des vulnérabilités de pointe de Qualys qui est intégré à une puissante solution de mise en conformité de l'activité informatique, à une analyse complète des applications Web et à des services de détection des codes malveillants.

**À l'aide d'une seule et même plate-forme de gestion de la sécurité, les entreprises peuvent :**

- ✓ Définir des politiques pour établir une infrastructure informatique fiable et conforme à la bonne gouvernance et aux meilleures pratiques.
- ✓ Automatiser les évaluations de sécurité permanentes et gérer efficacement les risques de vulnérabilités sur les systèmes et les applications.
- ✓ Atténuer les risques et éliminer les menaces en appliquant la gestion des vulnérabilités la plus réputée du marché.
- ✓ Surveiller et mesurer la conformité informatique depuis une même console unifiée pour gagner du temps et réduire les coûts.
- ✓ Distribuer des rapports de sécurité et de conformité personnalisés pour répondre aux besoins uniques des RSSI, des dirigeants, des auditeurs et autres professionnels de la sécurité.

## VUE INTÉGRÉE DE LA SÉCURITÉ ET DE LA CONFORMITÉ INFORMATIQUE

Pour les RSSI aux ressources humaines et financières limitées, QualysGuard Security and Compliance Suite permet aux équipes d'audit réseau et de conformité d'exploiter efficacement les informations clés concernant la sécurité informatique de l'entreprise. Avec une même suite consolidée, des groupes aux responsabilités différentes peuvent utiliser ces mêmes informations pour répondre à leurs besoins spécifiques.
La solution QualysGuard Security and Compliance Suite automatise le processus de gestion des vulnérabilités et de conformité aux politiques à travers l'entreprise grâce à la découverte et à la cartographie du réseau, à la classification des actifs par priorité, au reporting de l'évaluation des vulnérabilités et au suivi de la remédiation, le tout en fonction des risques pour l'activité de l'entreprise. Grâce aux fonctionnalités de conformité aux politiques de cette offre, les responsables de la sécurité peuvent auditer, appliquer et renseigner la conformité aux politiques de sécurité interne et à la réglementation externe.

**Les principaux composants de QualysGuard Security and Compliance Suite sont :**

### QualysGuard Vulnerability Management
Gestion évolutive des risques de sécurité et des vulnérabilités déployable à l'échelle mondiale

### QualysGuard Policy Compliance
Définition, audit et renseignement sur la conformité en matière de sécurité informatique

### QualysGuard PCI Compliance
Validation automatisée de la conformité PCI pour les commerçants et les acquiring banks

### QualysGuard Web Application Scanning
Évaluation et reporting automatisés de la sécurité des applications Web qui évoluent avec votre activité

### QualysGuard Malware Detection
Service gratuit de détection des codes malveillants pour les sites Web

### Qualys SECURE Seal
Service de test de sécurité et sceau de sécurité pour sites Web qui analyse les vulnérabilités, les codes malveillants et valide le certificat SSL


L'offre QualysGuard IT Security & Compliance Suite

## QUALYSGUARD REPOND AUX BESOINS DU RSSI D'AUJOURD'HUI

Qualys a basé son service sur la détection et le reporting efficaces des vulnérabilités sur l'ensemble de l'infrastructure de l'entreprise. Dans la mesure où les vulnérabilités connues sont relativement peu nombreuses par rapport aux « exploits » connus, il est raisonnable de donner la priorité à la découverte et à la correction des vulnérabilités plutôt qu'à la lutte contre chaque « exploit » potentiel ou code malveillant récemment développé. QualysGuard est la réponse idéale aux défis d'aujourd'hui car elle garantit sans peine un environnement sécurisé et conforme.

QUALYS®

**QualysGuard soutient le RSSI d'aujourd'hui comme suit :**

- **Visibilité universelle de l'état de la sécurité informatique et de la conformité de l'entreprise**
  Les fonctionnalités de déploiement mondial hautement évolutives de QualysGuard associées à une base de données centralisée des résultats offrent davantage de transparence au RSSI concernant les risques pour les systèmes informatiques et la capacité de remédier rapidement les systèmes non conformes.
- **Innovation métier**
  Le RSSI peut facilement ajouter de nouvelles applications et activités au programme de gestion des vulnérabilités et de la conformité de Qualys, sans contraintes pour l'infrastructure métier.
- **Mise à niveau de l'infrastructure technique**
  Le RSSI peut garantir la conformité et la détection des codes malveillants pour de nouveaux environnements d'exploitation et applications. Apportant de la valeur à l'infrastructure qui évolue, le service de sécurité Qualys permet au RSSI de planifier un changement évolutif vers la technologie qui soutient l'activité.
- **Réduction du coût de la sécurité**
  Qualys n'exige aucun investissement en amont dans du personnel ou des équipements. Le service est facturé en fonction du nombre d'analyses requises et de l'étendue de l'analyse des vulnérabilités. Le RSSI contrôle la fréquence d'utilisation du service Qualys.
- **atives socialement gratifiantes**
  La sécurité dans les nuages est l'un des principaux facteurs qui contribuent aux initiatives Green IT car des solutions comme Qualys évitent à la Direction informatique de dépenser de l'argent pour l'alimentation et le refroidissement de serveurs dédiés. En outre, la gestion des risques de sécurité et de la conformité pour les nouveaux modèles informatiques dans les nuages est optimisée.
- **Adoption de solutions tactiques**
  Quel que soit le niveau de planification dans l'entreprise, il y aura toujours la découverte d'une nouvelle application ou la fusion avec une autre entreprise qui obligera l'équipe chargé de la sécurité à évaluer rapidement un environnement technique par rapport aux recommandations de conformité. Grâce au service Qualys, le RSSI peut procéder à cette évaluation et obtenir un rapport opérationnel en quelques heures seulement, depuis n'importe où dans le monde.
- **Promotion d'initiatives stratégiques**
  L'utilisation du service Qualys est un outil stratégique pour bâtir un programme de gestion des risques de sécurité informatique et de la conformité. Une fois en service, ce dernier peut valider automatiquement la résilience de l'infrastructure de l'entreprise face aux toutes dernières menaces les plus sophistiquées.

Il est évident que le SaaS et l'informatique dans les nuages transforment de façon positive l'infrastructure informatique. Et lorsque les RSSI choisissent les meilleurs fournisseurs SaaS possibles, ils peuvent résoudre de nombreux problèmes de sécurité natifs tandis que les services de sécurité en mode SaaS les aident à maintenir la sécurité de leurs données et à optimiser le fonctionnement et le coût de leurs systèmes tout en se conformant à la réglementation.

*Les études de cas présentées à la fin du présent document sont des exemples d'entreprises de premier ordre qui s'appuient sur cette évolution vers les nuages pour atteindre leurs objectifs en matière de sécurité et de conformité.*

***Pour en savoir plus sur Qualys et tester QualysGuard IT Security & Compliance Suite, rendez-vous sur : www.qualys.com.***

# Annexe

**ETUDE DE CAS : SODEXO**

**ETUDE DE CAS : CARREFOUR**

**ETUDE DE CAS : MCDONALD'S FRANCE**

# SODEXO RENFORCE LA SÉCURITÉ DES SI DE SES FILIALES AVEC QUALYSGUARD

*"Cinq ans plus tard nous utilisons toujours la même solution, mais sur un périmètre, géographique et fonctionnel, beaucoup plus vaste. C'est la force du modèle Software as a Service que d'avoir su tenir compte et intégrer, de manière continue et transparente pour nous, l'évolution de nos besoins spécifiques, ainsi que ceux du marché en général."*

Abdellah Cherkaoui,
Chief Information Security Officer
**Sodexo**

**Compléter les audits sur site ponctuels par une analyse automatisée et continue des vulnérabilités de chaque filiale.**

C'était le tonneau des danaïdes : après avoir audité et aidé les équipes de ses trente filiales dans le monde à améliorer la sécurité de leur SI, l'équipe d'audit Groupe de Sodexo Chèques & Cartes de Services (CCS) ne pouvait matériellement pas répéter l'exercice plus d'une fois tous les deux ans, en moyenne. "*Entre temps, les configurations des SI ayant évolué au rythme rapide imposé par les besoins du métier et de nos clients, il était souvent nécessaire de reprendre à zéro*", explique Abdellah Cherkaoui, Chief Information Security Officer de l'activité CCS du Groupe. Certes, l'audit sur site offrait une vision détaillée du niveau de sécurité des SI de la filiale, ainsi qu'une liste de recommandations pour l'améliorer, mais un tel fonctionnement pouvait difficilement s'adapter à la croissance soutenue de l'activité et à l'apparition de nouvelles filiales, et encore moins offrir au siège une vision immédiate de son exposition au risque. "*Nous ne pouvions pas faire d'audits plus fréquents, et nous ne souhaitions pas mettre en place des équipes locales, qui n'auraient alors plus été indépendantes de la filiale à auditer*", poursuit Abdellah Cherkaoui. Il fallait donc trouver autre chose.

Le Groupe s'est alors mis en quête d'une solution technique capable de seconder l'équipe d'audit entre deux passages et offrir ainsi une vision continue de l'exposition des filiales. Cela relève cependant du grand écart fonctionnel : la solution doit être capable de s'adapter à toutes les filiales, de la plus grosse qui réalise à elle seule une part importante du volume d'émission de l'activité jusqu'à la plus petite. "*Mais une solution simple adaptée à cette dernière ne sera pas nécessairement assez complète pour répondre aux besoins de la première, et vice-versa*", observe le responsable de la sécurité. De plus, la solution doit également pouvoir être administrée simplement, et permettre une vue centralisée du niveau de risque et de la gestion des vulnérabilités des SI des filiales, sans toutefois nécessiter de présence locale dédiée dans la filiale. Enfin, la solution doit apporter des recommandations effectives et continuellement mises à jour, permettant aux équipes locales de corriger les vulnérabilités au fur et à mesure de leurs apparitions.

"*Nous avons fait le tour du marché, où s'opposaient l'approche logicielle et celle de Software as a Service. Mais nous avions décidé de commencer par analyser notre exposition depuis l'extérieur, et le modèle SaaS nous semblait le plus adapté pour cela. Bien entendu le fait de n'avoir rien à déployer en interne ni aucune organisation à créer pour supporter la solution a également joué en la faveur de ce modèle*", justifie Abdellah Cherkaoui.

## Modéliser l'organisation de l'entreprise

Les équipes chargées du projet identifient alors plusieurs solutions basées sur le mode SaaS afin de choisir celle qu'ils évalueront de manière plus approfondie. "*De toutes les solutions étudiées, celle de Qualys était en avance sur deux points : d'abord par son interface, qui permettait une organisation très flexible et très adaptable, par exemple par filiale, par type d'équipements ou encore par niveau de risque. Cette flexibilité de l'interface nous permettait de vraiment coller à notre organisation géographique. Ce service se distinguait ensuite par la qualité de ses rapports très diversifiés, très granulaires, ainsi que par l'offre de recommandations précises pour la correction des vulnérabilités. Ce dernier point est vital pour des équipes locales avec des compétences sécurité limitées. Elles peuvent prendre le rapport tel quel et savoir ce qu'elles doivent faire et où trouver l'information complémentaire si nécessaire.*", poursuit le CISO.

Sodexo demande alors une licence d'évaluation et met le service à l'épreuve du terrain. "*Nous avons tout simplement comparé les résultats des analyses aux rapports très complets*

*fournis par notre équipe d'audit*". Et le résultat est à la hauteur des attentes de l'équipe en termes de qualité d'analyse. Mais il reste toutefois un dernier frein au déploiement : la crainte de voir des données confidentielles hébergées par un prestataire externe. Une intrusion chez le prestataire ou une malveillance interne pourrait en effet révéler la totalité des points vulnérables de l'architecture de Sodexo.

"*Nous avons mené une analyse de risque afin d'évaluer l'impact de la perte de notre liste de vulnérabilités par rapport au gain que le service nous offre. Car il faut être réaliste : le fait d'avoir une liste de vulnérabilités chiffrée chez un prestataire reconnu dont c'est le coeur de métier est largement moins risqué que de rester avec des vulnérabilités béantes comme c'était le cas à l'époque*", admet Abdellah Cherkaoui. Par ailleurs, Sodexo a décidé d'auditer Qualys. "*Nous avons procédé à des visites sur site et exigé de consulter les rapports d'audits indépendant déjà réalisés. Nous avons été rassurés par les contrôles internes mis en place, et par le fait que toutes les données clients sont chiffrées par la clé privée de ces derniers. Personne chez Qualys ne peut lire nos données de vulnérabilités*", explique le responsable sécurité.

## Un service offert aux filiales

Une fois la décision prise, la mise en oeuvre du service s'avère rapide. Après avoir acquis une licence pour une centaine d'adresses IP, l'équipe Sodexo modélise petit à petit l'organisation du groupe dans l'interface d'administration et programme les analyses de tous leurs points d'accès externes. Bien que la configuration de l'outil soit centralisée, le rapport, en revanche, est entièrement destiné aux filiales. "C'est une vente ! Nous avons dit aux filiales "*ce rapport est pour vous. Je vous apporte un outil local, vous ne le payez pas. Cela va vous expliquer comment régler vos vulnérabilités. Toutes les mises à jour sont prises en charge, vous n'avez qu'à identifier vos frontaux. Et nous, on continue à vous supporter par des audits techniques sur site comme d'habitude*", explique Abdellah Cherkaoui. Et les filiales vont se prendre au jeu. Elles s'approprieront rapidement l'outil, aussi bien lors d'analyses régulières que pour la mise en ligne de nouveaux serveurs. Et il sera apprécié au point que certaines filiales décident de s'offrir les services de consultants externes afin de les aider à corriger leurs vulnérabilités plus efficacement.

De son côté, le siège surveille les tendances depuis l'interface centralisée. "La règle est qu'une vulnérabilité de niveau 4 ou 5 (urgente ou critique) ne doit pas rester sans correction plus d'un mois. De plus, grâce aux améliorations apportées, l'outil devient de plus en plus pointu et précieux, car il peut procéder aujourd'hui à une certaine corrélation qui permet de mieux noter l'importance des vulnérabilités : une faille critique qui aurait comme pré-requis l'exploitation d'une vulnérabilité inexistante serait par exemple rétrogradée", poursuit Abdellah Cherkaoui.

## L'émergence de nouveaux besoins

Au fil de l'utilisation du service, deux besoins nouveaux ont émergés : l'analyse des systèmes internes, d'abord. "*Le demande est venue des filiales. A ce moment, Qualys proposait une appliance à déployer sur le LAN, que nous avons décidé de tester. Et entre des configurations laissées par défaut ou des correctifs non appliqués, nous avons immédiatement vu l'intérêt du boîtier !*", reconnaît le CISO. Sodexo décide alors de déployer une appliance par filiale, à la condition que ces dernières s'engagent à agir sur les rapports d'analyses internes et à obtenir une décrue de leurs vulnérabilités internes.

Dernier besoin nouveau, enfin, le respect de la réglementation Sarbanes-Oxley et du contrôle interne. "*Nous avons identifié une quinzaine de contrôles essentiels. Nous avons rapidement vu que Qualys pouvait aider les filiales à automatiser et rendre le suivi de certains des contrôles beaucoup plus simple et effectif. Un exemple très parlant est celui de la gestion des configurations par défaut. Nous avons, grâce à Qualys, pu créer un modèle de rapport personnalisé qui ne présente que ces configurations par défaut, que nous avons ensuite partagé instantanément avec toutes les filiales*", explique Abdellah Cherkaoui, avant de conclure "*C'est la force du modèle SaaS : nous utilisons toujours le même produit depuis cinq ans, mais il a su s'adapter à nos nouveaux besoins*".

### LE METIER

Avec 310.000 entreprises et institutions clientes, 20,2 millions d'utilisateurs et plus de 1 million de partenaires affiliés dans 30 pays, le Groupe Sodexo est le numéro 2 mondial de l'activité Chèques et Cartes de Services.

### LE PERIMETRE

Répondant aux besoins et contraintes locales, les Systèmes d'Information des filiales de Sodexo Chèques & Cartes de Services sont à l'image de ses implantations: hétérogènes, souvent multi-vendeurs et multi plates-formes.

### LE PROBLEME

Le Groupe souhaitait améliorer sa connaissance et la gestion des vulnérabilités de tous ces Systèmes d'Information distribués, réparti à travers la planète au sein de filiales très décentralisées.

### LE DEFI OPERATIONNEL

Des audits techniques sur site sont réalisés en moyenne une fois tous les deux ans, ce qui est largement insuffisant pour suivre de manière efficace les vulnérabilités et leur correction. Une présence locale dédiée à l'audit n'est cependant pas imaginable, car elle serait difficilement indépendante de la production. De plus, les ressources locales sont concentrées sur le support quotidien des opérations, n'ayant souvent ni le temps ni les compétences nécessaires pour découvrir, analyser et corriger les vulnérabilités des SI.

### LA SOLUTION

QualysGuard Enterprise, solution on demand de Qualys, délivrée en mode « Software as a Service » (SaaS) et associée à des boitiers « plug-and-play » au sein de chaque filiale. Analyse illimitée et à la demande de tous les équipements présents sur le réseau, du routeur à la base de donnée en passant par les serveurs et les stations de travail, multi-vendeur, multi-plate-forme.

### POURQUOI QUALYS ?

- Qualité, richesse et souplesse des rapports d'analyse
- Capacité à modéliser l'organisation du Groupe dans l'interface de la solution
- Sécurité de la plate-forme chez Qualys pour y héberger des données confidentielles
- Pertinence des analyses de vulnérabilité
- Source directe de connaissance pour les ressources locales des filiales du Groupe

### SITE WEB

http://www.sodexo.com

QUALYS®
www.qualys.com

**USA – Qualys, Inc.**
1600 Bridge Parkway
Redwood Shores
CA 94065
Tél. : 1 (650) 801 6100
sales@qualys.com

**Royaume-Uni – Qualys, Ltd.**
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
Tél. : +44 (0) 1753 872101

**Allemagne – Qualys GmbH**
Aéroport de Munich
Terminalstrasse Mitte 18
85356 Munich
Tél. : +49 (0) 89 97007 146

**France – Qualys Technologies**
Maison de la Défense
7, Place de la Défense
92400 Courbevoie
Tél. : +33 (0) 1 41 97 35 70

ON DEMAND SECURITY

groupecarrefour

# QualysGuard pour Animer la Communauté Sécurité

> ***"Nous avons obtenu des indicateurs compréhensibles par les non-informaticiens, et donc pu pousser la sécurité auprès des managers qui ne sont pas techniques."***

Nicolas Burtin, Responsable SSI, **Groupe Carrefour**

Le groupe Carrefour a déployé des boîtiers QualysGuard afin d'auditer ses vulnérabilités sur le WAN (Wide Area Network). A l'heure du bilan, la solution permet non seulement de mesurer le niveau d'exposition de manière quantifiable, mais elle est aussi devenue un lien entre les responsables sécurité du groupe.

Le groupe Carrefour, organisé en de nombreuses Business Units, exploite un WAN important. Dans le courant de l'année 2007, le Groupe Carrefour décide de renforcer son analyse des vulnérabilités. "*Nous souhaitions connaître de manière quantifiable notre exposition à ce type de risques*", indique Nicolas Burtin, en charge de ces aspects au sein de la Direction de la Sécurité des Systèmes d'Information du Groupe Carrefour.

La DSSI Groupe procède alors à une évaluation du marché en commençant par les logiciels libres d'analyse des vulnérabilités dont l'industrialisation s'avère rapidement insuffisante. Des produits commerciaux, à déployer en local, sont également considérés. "*Le fait qu'il s'agisse d'outils locaux nous rassurait, car externaliser les données sécurité nous semblait antinomique !*", reconnaît Nicolas Burtin. Mais les solutions étudiées manquent d'ergonomie et relèvent des soucis d'installation durant la phase de maquette.

## Externaliser la sécurité

"*Une solution Software as a Service, à l'inverse, nous paraissait très souple tant en termes de déploiement que d'utilisation. Mais il restait le problème de l'externalisation. Après une série d'échanges avec la société Qualys, nous avons été convaincus que la confidentialité était au rendez-vous*", détaille Nicolas Burtin. Seul regret : l'incapacité, pour le moment, d'utiliser les clés de chiffrement générées par Carrefour à la place de celles fournies par Qualys.

Contrairement à de nombreuses entreprises qui choisissent de commencer par analyser une portion réduite de leur infrastructure, le Groupe Carrefour a préféré des analyses moins nombreuses mais plus vastes. Un choix qui montrera tout son intérêt à l'heure du bilan.

La solution a beau être en mode SaaS, analyser un réseau privé exige la présence des boîtiers sur l'infrastructure. "*Cela s'est fait très simplement : j'ai remis la mallette contenant le boîtier aux RSSI des BU qui devaient avoir leur propre appliance, lors de leur passage à Paris. Une fois les boîtiers installés, ils sont gérés automatiquement par des comptes distincts créés à l'avance*", souligne Nicolas Burtin.

## Une utilisation à plusieurs niveaux

Les analyses conduites régulièrement génèrent une masse d'information qu'il faut traiter. C'est là que l'organisation mise en place par la DSSI Groupe de Carrefour parvient à créer du lien avec la communauté des RSSI locaux et à renforcer le rôle de ces derniers auprès des DSI locales.

"*Nous trions les informations remontées afin d'isoler les vulnérabilités les plus critiques (de niveaux 4 et 5) et parmi elles, celles qui sont les plus nombreuses. Cela nous donne une liste plus courte que nous envoyons au RSSI du pays ou de la BU en question, qui peut alors l'étudier avec la DSI locale. Car l'objectif est aussi de créer le lien entre le RSSI et l'opérationnel*", explique Nicolas Burtin.
De même, le suivi des améliorations est fait de telle sorte qu'il implique fortement le RSSI local : le Groupe procède à des revues régulières avec chaque pays afin d'évoquer les actions nécessaires et consulte les statistiques QualysGuard relatives à la Business Unit en question. "*Mais pour le reste, c'est localement que chaque RSSI détermine les priorités.*

*C'est un moyen de responsabiliser les RSSI locaux, et de faire en sorte qu'ils s'approprient l'infrastructure. On a simplement établi avec eux la liste des actifs critiques, et ils doivent y veiller*", poursuit Nicolas Burtin.

Après un an d'exploitation, la solution QualysGuard a désormais "fait le tour du monde" chez Carrefour, en analysant l'Amérique, l'Europe et l'Asie. Au total, environ 500.000 adresses IP ont été détectées durant la phase de cartographie du réseau, et 16.000 d'entre elles constituent le périmètre à analyser. Carrefour est parvenu à réduire de 20% le nombre de ses vulnérabilités cette première année.

Certes, la DSSI convient qu'il aurait été plus facile de démarrer sur un périmètre plus réduit, et donc plus facile à maîtriser. "*Mais nous avons fait d'emblée le choix d'un périmètre large car nous voulions obtenir aussi un véritable effet de sensibilisation. Stratégiquement, ce projet n'aurait pas eu le même impact s'il avait été mené sur un périmètre réduit*", justifie Nicolas Burtin.

Car l'objectif de la DSSI Groupe était aussi de crédibiliser la sécurité auprès des autres interlocuteurs du SI : "*Il fallait montrer que les vulnérabilités constituent un problème concret et faire la démonstration que cet outil pouvait aider à le régler. Et cela ne peut se faire à petite échelle, ou du moins ça n'aurait pas marqué les esprits de la même manière. Alors que désormais tous les RSSI sont impliqués et nous avons pu obtenir des indicateurs clairs, accessibles aux non-informaticiens. Cela nous permet donc aussi de pousser le rôle de la sécurité auprès des managers qui ne sont pas de culture technique*", conclut Nicolas Burtin.

Au delà de la seule gestion des vulnérabilités, c'est ainsi une véritable opération de communication que la DSSI Groupe a pu mener, aussi bien auprès de ses RSSI locaux que des responsables métiers.

## LE METIER

Le groupe Carrefour est l'un des premiers acteurs de la grande distribution dans le monde (premier distributeur européen et second dans le monde). Le groupe compte 15.000 magasins, depuis les enseignes de proximité jusqu'aux hypermarchés.

## LE PERIMETRE

Le groupe Carrefour est organisé en Business Units réparties à travers le monde : chaque pays est une BU, ainsi que certaines entités spéciales, telle la branche Hypermarchés France ou l'entité Groupe elle-même. Toutes communiquent à travers un réseau mondial de type WAN.

## LE PROBLEME

Carrefour souhaitait formaliser sa gestion des vulnérabilités et disposer d'indicateurs clairs de son exposition aux risques sur son réseau interne WAN.

## LE DEFI OPERATIONNEL

La solution devait permettre d'impliquer les RSSI locaux, valoriser leur rôle auprès des DSI locales et souligner l'importance de la sécurité auprès des responsables non techniques

## LA SOLUTION

Quatre boîtiers QualysGuard Enterprise.

## POURQUOI QUALYS ?

- Simplicité de déploiement et d'utilisation
- Qualité des analyses
- Mode Software as a Service
- Automatisation des rapports

## SITE WEB

http://www.carrefour.com

QUALYS®
www.qualys.com

**USA – Qualys, Inc.** • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
**Royaume-Uni – Qualys, Ltd.** • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101
**Allemagne – Qualys GmbH** • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
**France – Qualys Technologies** • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
**Japon – Qualys Japan K.K.** • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
**Hong Kong – Qualys Hong Kong Ltd.** • 2/F, Shui On Centre, 6-8 Harbour Road, Wanchai, Hong Kong • T: +852 2824 8488

ON DEMAND SECURITY

c'est tout ce que j'aime
i'm lovin' it

# McDonald's France se Conforme à la Réglementation en s'Appuyant sur une Gestion Automatisée, Précise et Pratique des Vulnérabilités

***"QualysGuard nous permet d'automatiser nos audits de vulnérabilités internes et externes. Disposant d'un rapport concis sur la manière dont les utilisateurs internes et externes peuvent voir nos systèmes, nous pouvons évaluer en permanence la conformité de nos systèmes par rapport à nos politiques internes et à la réglementation."***

Wilfried Delcambre, Responsable Systèmes et Sécurité
**McDonald's France**

Il est impossible de parler grande cuisine sans évoquer la France. McDonald's France peut aujourd'hui donner au monde entier quelques conseils en matière de restauration rapide et pratique. Multinationale pesant 20,5 milliards de dollars, McDonald's Corporation est le Numéro 1 des services de restauration rapide de qualité et compte plus de 30 000 restaurants à travers le monde. Sa filiale française s'emploie à concevoir et à construire ses restaurants pour qu'ils se fondent dans l'architecture locale. « Nous autres Français sommes très attachés à nos traditions gastronomiques mais nous aimons aussi ce qui est pratique », déclare Wilfried Delcambre, responsable de l'infrastructure informatique de McDonald's France.

S'ils apprécient la décoration raffinée des restaurants et l'accès Wi-Fi gratuit à Internet, les clients de McDonald's ne perçoivent pas toute la logistique que l'entreprise déploie en coulisses pour sécuriser les informations sur les cartes de crédit ainsi que ses propres informations financières et propriétaires. Un gros effort est fait pour veiller à protéger les systèmes d'exploitation, applications et serveurs contre les toutes dernières vulnérabilités logicielles et autres problèmes de configuration susceptibles de mettre en jeu la sécurité et la conformité à la réglementation de l'entreprise. Société cotée au NYSE (symbole : MCD), McDonald's doit veiller en permanence à ce que ses opérations soient conformes à la loi Sarbanes-Oxley Act de 2002 (SOX). Cette loi votée pour garantir la transparence et l'intégrité du reporting financier pour les entreprises cotées vise à responsabiliser davantage les dirigeants par rapport aux résultats financiers de leur société.

Les risques qui pèsent sur les initiatives de sécurité et de conformité à la réglementation ne cessent d'augmenter. En effet, les responsables chargés de la sécurité doivent faire face à une augmentation rapide du nombre de nouvelles vulnérabilités. Selon le centre de coordination des CERT, 3 780 vulnérabilités ont été rapportées en 2004. Ce nombre a plus que doublé pour atteindre 8 064 cas en 2006. « Il faut surveiller de manière cohérente les systèmes afin de pouvoir atténuer les problèmes. Il s'agit d'un processus sans fin, » explique M. Delcambre. Un système non patché ou mal configuré peut fragiliser le contrôle des systèmes financiers exigé par la Section 404 de la réglementation SOX et par la norme PCI DSS (Payment Card Industry Data Security Standard) de l'industrie de la carte bancaire. Cette norme PCI DSS définit les contrôles de sécurité pour le traitement et la gestion des informations et des transactions liées aux cartes de crédit. Ces contraintes, ainsi que d'autres dispositions légales et réglementations de l'industrie, exigent non seulement que les systèmes soient sécurisés, mais aussi que la sécurité puisse être prouvée au législateur et aux autorités chargées de réguler l'industrie.

Soucieux de se conformer dans ce domaine, McDonald's France a donc cherché un moyen pour automatiser nombre des processus liés à la gestion des risques et des vulnérabilités : découverte des systèmes, identification des vulnérabilités et remédiation. Wilfried Delcambre explique comment un conseiller informatique a recommandé QualysGuard® de Qualys® Inc. Avec QualysGuard, le contrôle de l'ensemble du cycle de vie de la gestion des vulnérabilités (découverte des actifs, évaluation des vulnérabilités, suivi des correctifs de sécurité) est rationalisé et respecte la législation en vigueur et la réglementation interne de l'entreprise. Totalement administrée par Qualys, cette solution à la demande est fournie en tant que service Web et ne nécessite le déploiement d'aucun logiciel ni d'aucune infrastructure coûteuse.

« Nous avions besoin d'une analyse à la fois externe et interne de notre sécurité. Et QualysGuard nous l'apporte de manière vraiment optimale. Cette solution nous permet d'identifier, de remédier et de suivre nos vulnérabilités », déclare M. Delcambre. En outre, la capacité de QualysGuard à automatiser les analyses permet à McDonald's de procéder à ces évaluations chaque semaine. « Grâce à QualysGuard, nous disposons d'une vue interne détaillée de l'ensemble de notre infrastructure ainsi que d'une vue découverte de nos systèmes depuis l'extérieur ».

Grâce à cet atout, l'entreprise peut non seulement garantir sa sécurité, mais aussi prouver que ses patches système sont conformes à la réglementation. « QualysGuard tient une part importante dans nos efforts de conformité », déclare M. Delcambre.

Enchantée par cette solution, McDonald's France s'intéresse désormais à QualysGuard PCI pour l'aider à justifier la sécurité de ses transactions par carte de crédit ainsi que la conformité à la norme PCI DSS (Payment Card Industry Data Security Standard). Définie par les principales sociétés de cartes de crédit, la norme PCI DSS exige des commerçants qu'ils garantissent le niveau de sécurité nécessaire pour protéger de manière adaptée les transactions et les données liées aux cartes de crédit. Cette norme impose douze exigences de sécurité, notamment l'installation d'un firewall réseau, le chiffrement des données du détenteur de la carte lors de ses déplacements, le suivi strict de l'authentification et de l'autorisation ainsi que l'existence d'un programme complet de gestion des vulnérabilités. Des pénalités sévères sont prévues en cas de non conformité. En effet, les commerçants qui ne se plient pas aux exigences de conformité, ou qui subissent une faille, pourront être interdits de traitement de transactions par carte de crédit, devront s'acquitter de frais de traitement supérieurs et payer des amendes pouvant atteindre jusqu'à 500 000 dollars pour chaque cas de non conformité.

« Nous testons actuellement QualysGuard PCI, une solution qui nous aidera à rationaliser les formulaires et les exigences de reporting et qui nous garantira que tout est en ordre pour la conformité PCI », explique M. Delcambre.

À l'instar de toutes les solutions de sécurité à la demande de Qualys, il n'y a rien à installer ou à déployer ni aucun coût caché. Avec QualysGuard PCI, les entreprises peuvent rationaliser les questionnaires et les évaluations de vulnérabilités exigés par l'industrie de la carte bancaire. Cette solution crée le rapport de validation requis, lequel peut être automatiquement soumis à la banque émettrice d'un commerçant en ligne. Wilfried Delcambre poursuit : « Nous comptons sur la solution QualysGuard PCI pour qu'elle nous fasse gagner du temps et qu'elle rende plus efficaces nos efforts de conformité PCI ».

Même si Qualys automatise de nombreux aspects de la gestion des vulnérabilités pour gagner du temps et améliorer les performances de l'équipe informatique de McDonald's France, M. Delcambre apprécie par dessus tout les niveaux de sécurité toujours plus élevés garantis par QualysGuard. « Vos systèmes ont beau être vraiment sécurisés, tant de l'intérieur que de l'extérieur, le moindre problème de configuration dans votre firewall peut vous exposer à des risques majeurs. C'est précisément ce problème, ainsi que de nombreux autres types de risques, que QualysGuard détecte à notre place ».

**PRESENTATION DE MC'DONALDS**
A l'international
Plus de 30 000 restaurants dans 127 pays

**IMPORTANCE ET TAILLE DE MCDONALD'S FRANCE**
45 000 employés et 1 084 restaurants

**ACTIVITÉ**
McDonald's est le premier restaurateur au monde avec plus de 30 000 restaurants de proximité implantés dans plus d'une centaine de pays. Près de 70% des restaurants McDonald's à travers le monde sont exploités localement et appartiennent à des entrepreneurs indépendants.

**PROBLÉMATIQUE MÉTIER**
Filiale de McDonald's Corporation, McDonald's France cherchait à automatiser ses évaluations des vulnérabilités pour garantir en permanence sa conformité tant aux stratégies de sécurité internes qu'aux réglementations, notamment à la législation Sarbanes-Oxley et à la norme Payment Card Industry Data Security Standard.

**SOLUTION**
McDonald's France a adopté le service à la demande QualysGuard et son appliance pour identifier automatiquement et corriger plus efficacement les vulnérabilités système et les problèmes de configuration.

**POURQUOI MCDONALD'S A CHOISI QUALYS ?**
- Taux de précision : 99,997 % basé sur plus de 150 millions d'audits IP par an.
- À la demande : Aucun logiciel d'infrastructure ou d'entreprise à déployer ni à maintenir.
- Ponctualité : Contrôles de sécurité et intelligence réseau toujours ponctuels.

**SITE WEB**
www.mcdonalds.com

QUALYS®
www.qualys.com

**USA – Qualys, Inc.**
1600 Bridge Parkway
Redwood Shores
CA 94065
Tél. : 1 (650) 801 6100
sales@qualys.com

**Royaume-Uni – Qualys, Ltd.**
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
Tél. : +44 (0) 1753 872101

**Allemagne – Qualys GmbH**
Aéroport de Munich
Terminalstrasse Mitte 18
85356 Munich
Tél. : +49 (0) 89 97007 146

**France – Qualys Technologies**
Maison de la Défense
7, Place de la Défense
92400 Courbevoie
Tél. : +33 (0) 1 41 97 35 70

ON DEMAND SECURITY