Sécurité & Conformité à l'ère du Cloud

QUALYS®

Sommaire

Introduction

Nous vivons désormais dans une ère où la technologie est omniprésente. Que cela soit à la maison, au bureau ou en déplacement, la majorité d'entre nous sommes connectés, où que nous soyons, non seulement avec des personnes mais aussi avec un large éventail d'informations et de technologies. Il est donc devenu difficile de dissocier temps de travail et temps libre, les mêmes équipements étant utilisés de manière interchangeable dans les deux contextes. Cette tendance indéniable est à la fois une source d'opportunités énormes, mais aussi de risques importants pour les entreprises qui adoptent la culture du « toujours connecté », que ce soit avec leurs clients, leurs partenaires ou leurs collaborateurs.

Des services technologiques sont consommés à tout moment et partout où cela s'impose tandis que les données associées peuvent être stockées n'importe où. Chez Qualys, nous sommes persuadés que les entreprises, sous peine d'être dépassées, doivent entrer dans l'« ère du Cloud ». Pour ce faire, elles doivent s'affranchir massivement des contraintes de l'architecture client/serveur, voire des applications Web de première génération, et favoriser l'essor d'un nouveau monde articulé autour de la connectivité qui améliorera les communications, la collaboration et la productivité.

Sécurité et conformité à l'ère du Cloud

Caractéristiques majeures de l'ère du Cloud :

Le navigateur comme pivot

Le navigateur Web est l'interface commune à Internet, aux applications métier et aux magasins de données. Il offre un accès universel à toutes les parties prenantes sur tout un ensemble d'équipements, y compris les ordinateurs personnels et les smartphones que possèdent à la fois l'entreprise et les employés (concept BYOD ou « Apportez votre propre matériel »). Et pourtant, les navigateurs contiennent des vulnérabilités qui peuvent provoquer des infections à base de codes malveillants, et ce en dépit des efforts fournis par les développeurs pour corriger et résoudre ces failles qui sont devenues la voie d'accès royale pour les pirates avides de capturer des informations, de subtiliser des identifiants/mots de passe ou de prendre le contrôle des équipements des utilisateurs.

Applications Web : le nouveau périmètre

Plus faciles à créer et à déployer, les applications Web représentent désormais le point d'accès principal aux réseaux et aux données de l'entreprise et remplacent de facto le périmètre traditionnel. Aujourd'hui, les entreprises doivent dépenser autant de temps et d'énergie à détecter, suivre et gérer les applications Web qu'elles en consacrent à leurs réseaux périmétriques classiques. L'importance de ces applications, ainsi que le volume et le caractère sensible de leurs données sous-jacentes, ont attiré la convoitise de pirates qui exploitent les faiblesses et les failles de configuration des applications Web pour dérober des données sensibles ou réduire la disponibilité des applications.

Accès universel aux données

Avec l'informatique dans le Cloud, les applications peuvent être composées de données provenant de n'importe où. Elles peuvent être hébergées dans tout un panel de magasins de données internes et dans le Cloud, ce qui impose des communications sécurisées entre ces différents sites. Bien que de nombreux fournisseurs d'applications dans le Cloud aient réalisé des investissements considérables dans la sécurité, les services Cloud, par définition, offrent aux entreprises une visibilité restreinte et un accès limité à l'architecture sous-jacente. Et ces restrictions empêchent les entreprises d'identifier les écarts potentiels et de vérifier l'efficacité de leur stratégie de sécurité.

La mondialisation est la norme et non pas l'exception

Le Cloud désintègre les frontières régionales et territoriales. Les données migrent d'un endroit vers un autre, les utilisateurs évoluent en toute transparence entre les différents sites tandis que les systèmes peuvent être administrés par un large éventail d'utilisateurs autorisés qui ne sont pas nécessairement vos employés. Tout ceci pose des problèmes d'ordre juridique, induit des besoins d'authentification, exige de la confiance et complique le reporting et l'attestation en matière de conformité.

Infrastructure hybride

Aucune société d'envergure ne peut abandonner ses systèmes internes du jour au lendemain, mais les entreprises font de gros efforts pour rendre ces ressources plus performantes grâce à la consolidation et à la virtualisation. Dans la mesure où l'infrastructure informatique restera dans un avenir proche une association de centres de données physiques classiques et de technologies dans le Cloud, des contrôles de sécurité doivent être appliqués et la conformité doit être documentée avec cohérence. Et ceci que les actifs technologiques se trouvent dans le centre de données de votre entreprise ou chez un fournisseur dans le Cloud situé n'importe où dans le monde.

La productivité, la souplesse et les avantages économiques du Cloud computing justifient l'adoption massive de services dans le Cloud, quels que soient les risques et la complexité encourus. Aussi, regardons d'un plus peu près les défis introduits à l'ère du Cloud pour chaque département informatique.

Défis de sécurité et de conformité à l'ère du Cloud

La sécurité est une bataille que votre entreprise ne peut pas gagner. En effet, le succès se mesure généralement à la capacité de maintenir les entreprises hors d'affaires médiatiques et les dirigeants des entreprises hors de prison. Une réalité de plus en plus basée sur le Web et l'adoption croissante de nouvelles infrastructures dans le Cloud et hybrides compliquent la tâche du professionnel de la sécurité.

Sécurité à l'échelle du Cloud

Comme décrit par la Cloud Security Alliance, l'une des caractéristiques essentielles du Cloud est son « élasticité rapide » . Le Cloud peut se développer aussi vite que votre entreprise l'exige. Hier encore, les équipements devaient être fournis, dimensionnés et installés, ce qui donnait à l'entreprise le temps de protéger les nouveaux équipements. Aujourd'hui, dimensionner une nouvelle instance de Cloud ne prend que quelques minutes et crée des problèmes en termes de visibilité (quels équipements sont réellement présents à un moment donné ?) et de contrôle (comment garantir l'application de configurations et de contrôles appropriés sur les nouvelles ressources ?).

Augmentation de la surface d'attaque

Avec les applications Web qui émergent comme le « nouveau périmètre », les entreprises doivent se faire à l'idée qu'elles ont autant de périmètres que d'applications Web. Associée au développement de la sous-traitance et des partenariats commerciaux, cette nouvelle tendance augmente fortement la surface d'attaque. Cette croissance exponentielle des cibles, y compris les bases de données, les postes de travail, les équipements mobiles, les routeurs, les serveurs et les commutateurs, fait littéralement exploser le nombre de vulnérabilités de sécurité et donne potentiellement aux pirates un accès non autorisé aux systèmes informatiques. Bâtir un puissant périmètre de sécurité du réseau tout en négligeant la sécurité des réseaux et des équipements internes n'est plus acceptable.

Optimisation des contrôles de sécurité existants

Les entreprises ont toujours déployé des produits de sécurité de niche pour résoudre des problèmes de sécurité spécifiques. Cependant, cette approche ne fournit pas systématiquement un état actualisé, précis et global de la sécurité et de la conformité de l'entreprise. À mesure que les infrastructures informatiques évoluent et intègrent un mélange de ressources sur site, dans le Cloud et hybrides, ces produits de sécurité spécifiques exécutés sur site mettent les entreprises au défi de pouvoir produire un inventaire complet et précis de leurs actifs et de leurs configurations informatiques, ce qui les empêche de protéger efficacement leur infrastructure contre les menaces à l'ère du Cloud.

Sécurisation des équipements légers

L'évolution de la technologie liée aux smartphones a engendré des systèmes d'exploitation mobiles plus sophistiqués et sécurisés, verrouillés par défaut, mais qui offrent cependant une visibilité et un contrôle limités du cœur du système d'exploitation. Les techniques d'hier pour lutter contre les codes malveillants au niveau du noyau ne sont plus adaptées. Tandis que le vol de données et les codes malveillants continuent d'infester ces équipements, les entreprises doivent envisager différentes méthodes pour fournir une sécurité suffisante à ces équipements.

Hiérarchisation des activités de sécurité

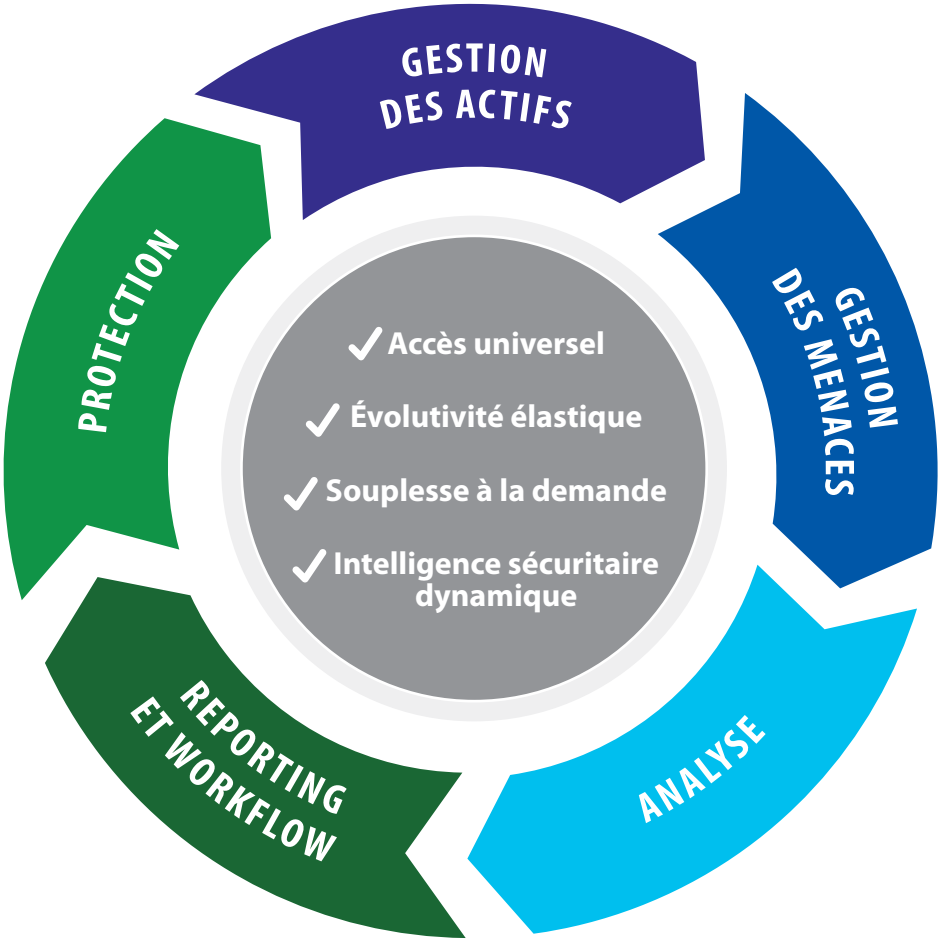
En raison des contraintes permanentes en termes de financement, de ressources et d'expertise, nombreuses sont les entreprises qui rencontrent des difficultés pour assurer leur protection à l'ère du Cloud, si bien qu'une sécurité performante est désormais conditionnée par une sélection attentive des activités à réaliser. L'ère du Cloud complique ces décisions et contraint les entreprises à hiérarchiser leurs activités de sécurité auprès d'un certain nombre de prestataires de services et de collaborateurs internes/externes qui peuvent échapper à leur contrôle. Qui plus est, comme il est dans la nature dynamique des pirates de lancer de nouvelles attaques qui exigent une réaction immédiate, les plans les mieux préparés peuvent rapidement devenir caduques.

Reporting de la conformité

L'un des effets malheureux des incidents de sécurité est le développement d'un environnement réglementaire et de conformité de plus en plus contraignant. Étant donné la nature mondialisée de l'essentiel de l'activité économique à l'ère du Cloud, votre entreprise doit probablement se conformer aux réglementations et politiques de nombreuses autorités nationales et locales, lesquelles se superposent et évoluent souvent. La conformité à ces différentes réglementations exige des mesures à la fois coûteuses et chronophages qui ont de lourdes conséquences financières et notamment pour la réputation de l'entreprise en cas de non conformité. Revised International Capital Framework (Bâle II), Health Insurance Portability and Accountability Act (HIPAA), North American Electric Reliability Corporation Standards (NERC), Payment Card Industry Data Security Standards (PCI DSS) et Sarbanes-Oxley Act de 2002 (SOX) sont quelques exemples de réglementations externes. Une enquête réalisée par le cabinet Gartner en 2011 estime qu'il en coûte en moyenne 1,7 million de dollars aux entreprises pour se conformer à la seule réglementation PCI DSS.

La plate-forme de sécurité dans le Cloud :

Poser les bases de la sécurité et de la conformité à l'ère du Cloud



Les solutions sur site client d'aujourd'hui ne sont pas en mesure de répondre aux besoins de sécurité et de conformité à l'ère du Cloud. Une nouvelle solution s'impose donc.

Caractéristiques essentielles d'une plate-forme Cloud :

Accès universel

Vos employés, fournisseurs de services et clients peuvent se trouver n'importe où et votre plate-forme de sécurité dans le Cloud doit être accessible partout et à tout moment.

Évolutivité élastique

À l'ère du Cloud, la fonction de sécurité et de conformité doit être aussi élastique et évolutive que le Cloud lui-même. À mesure que l'infrastructure informatique de votre entreprise se développe, la plate-forme que vous utilisez pour la sécuriser doit se développer progressivement.

Souplesse à la demande

Cette plate-forme doit être assez souple pour fournir à votre entreprise uniquement ce dont elle a besoin, au bon moment, et facturer seulement ce qui est véritablement utilisé.

Intelligence sécuritaire dynamique

Luttant en permanence contre des attaques sophistiquées et qui ne cessent d'évoluer, la plate-forme de sécurité dans le Cloud doit être actualisée de manière dynamique au moyen des informations les plus récentes sur les vulnérabilités, les configurations et les codes malveillants. Ainsi, votre entreprise pourra réagir plus rapidement aux menaces émergentes.

La plate-forme de sécurité et de conformité dans le Cloud doit offrir les fonctionnalités suivantes pour répondre aux besoins des entreprises actuelles :

Gestion des actifs

Votre entreprise ne peut pas protéger les actifs qu'elle ne connaît pas. En outre, la valeur de l'actif pour votre entreprise doit être prise en compte pour définir les priorités. Par conséquent, la plate-forme doit disposer de puissantes fonctionnalités de gestion des actifs.

Gestion des menaces

La plate-forme doit être capable d'analyser les vulnérabilités, d'évaluer et de surveiller les configurations et de déterminer les risques d'une attaque pour l'entreprise. Dans les environnements informatiques hybrides, la plate-forme doit fournir une vue unique du centre de données traditionnel et des environnements Cloud privés/publics sur une multitude d'équipements et sur la couche applicative.

Analyse

Pour faciliter la hiérarchisation des activités et combattre les attaques sophistiquées, il est impératif de collecter des informations exploitables auprès d'un éventail de sources de données. La plate-forme doit pouvoir analyser les données et fournir une vue claire des informations aux administrateurs chargés de la sécurité et de prendre des décisions sur le champ.

Reporting et workflow

Vu le nombre croissant d'obligations réglementaires dans les différentes régions et juridictions du monde, la plate-forme doit pouvoir fournir un ensemble commun de rapports à travers l'entreprise, gérer n'importe quel régime de reporting réglementaire et prendre en charge les workflows au sein de l'entreprise à l'heure où l'externalisation des opérations de sécurité s'accélère.

Protection

Afin de pouvoir contrer une attaque tout en réduisant au minimum le nombre de faux positifs, la plate-forme doit fournir une protection directe ou s'intégrer à d'autres défenses actives, parmi lesquelles des pare-feux pour applications Web (« WAF – Web Application Firewall »), des systèmes de prévention des intrusions et des pare-feux de dernière génération.

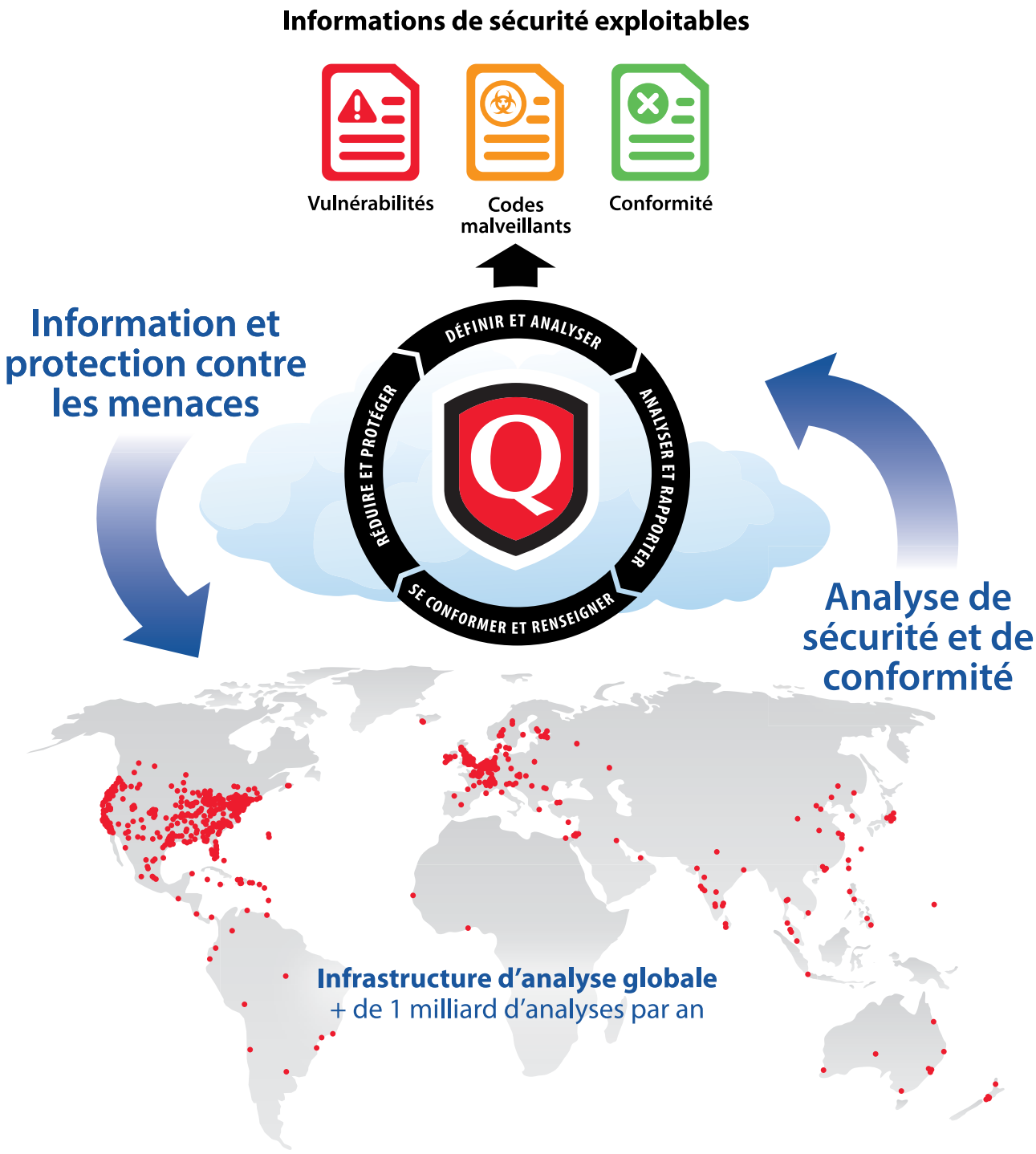
Bâtir une plate-forme de sécurité dans le Cloud ne se fait pas du jour au lendemain. En fait, il faut plus de 10 ans pour atteindre la masse critique, la présence globale, l'intelligence sécuritaire ainsi que l'expertise de renommée mondiale nécessaires. À l'ère du Cloud, un seul fournisseur est vraiment en mesure de répondre aux besoins de sécurité et de conformité des entreprises : Qualys.

Assurer la sécurité et la conformité à l'ère du Cloud

Qualys a été fondée en 1999, à l'apogée de la bulle Internet, lorsque la sécurité sur Internet commençait tout juste à préoccuper les dirigeants des entreprises. En décembre 2000, la société est devenue l'un des pionniers sur le marché de la gestion des vulnérabilités. Portée par une puissante association de technologies d'analyse très précises, faciles à utiliser et fournies via le Web, Qualys a développé l'utilisation du « logiciel fourni sous la forme de service » (SaaS) pour résoudre les problèmes de sécurité et de conformité d'entreprises de toute taille.

Le cœur de Qualys est la plate-forme dans le Cloud QualysGuard qui fournit une suite intégrée de solutions pour automatiser le cycle de vie de la découverte des actifs, de l'évaluation de la sécurité ainsi que de la gestion de la conformité de l'infrastructure et des actifs informatiques de l'entreprise. Et ce, que ces éléments résident au sein-même de l'entreprise, dans son périmètre réseau ou dans le Cloud. Le modèle de fourniture dans le Cloud de QualysGuard peut être déployé facilement, rapidement et à une échelle globale. Il garantit une mise en œuvre plus rapide, une adoption plus large et un moindre coût total de possession par rapport aux traditionnels logiciels d'entreprise installés sur site. En déployant QualysGuard, les entreprises peuvent obtenir des informations de sécurité exploitables sur les vulnérabilités et les codes malveillants potentiellement présents dans leur infrastructure informatique et accélérer ainsi leur mise en conformité aux politiques internes et à la réglementation externe.

Les résultats parlent d'eux-mêmes. Au cours des 12 dernières années, Qualys a développé une base internationale de clients composée de plus de 6700 entreprises implantées dans plus de 100 pays et dont une majorité figure aux classements Forbes Global 100 et Fortune 100. Ces clients réalisent plus de 1 milliard d'audits/analyses IP par an.



L'ère du Cloud obligera les entreprises de toute nature et de n'importe quelle taille à protéger leur patrimoine informationnel critique de manière plus réactive. Fournissant des informations de sécurité exploitables, QualysGuard est et restera la plate-forme stratégique de gestion de la sécurité informatique et de la conformité de l'entreprise.

QUALYSGUARD® Cloud Platform

La plate-forme dans le Cloud QualysGuard offre une suite de solutions de gestion de la sécurité informatique et de la conformité qui s'appuient sur des services de base partagés et extensibles et sur une infrastructure Cloud multi-locataire hautement évolutive.

Infrastructure Cloud QualysGuard

L'infrastructure QualysGuard comprend les données, les ressources d'analyse, l'infrastructure logicielle et matérielle ainsi que les ressources de gestion d'infrastructure qui constituent le fondement de la plate-forme dans le Cloud. En voici certains aspects majeurs :

Capacité évolutive
L'infrastructure modulaire et évolutive de QualysGuard s'appuie sur des technologies de virtualisation et Cloud qui permettent d'allouer des ressources supplémentaires à la demande sur l'ensemble de notre plate-forme Cloud QualysGuard afin d'assurer le développement et l'évolutivité de nos solutions.

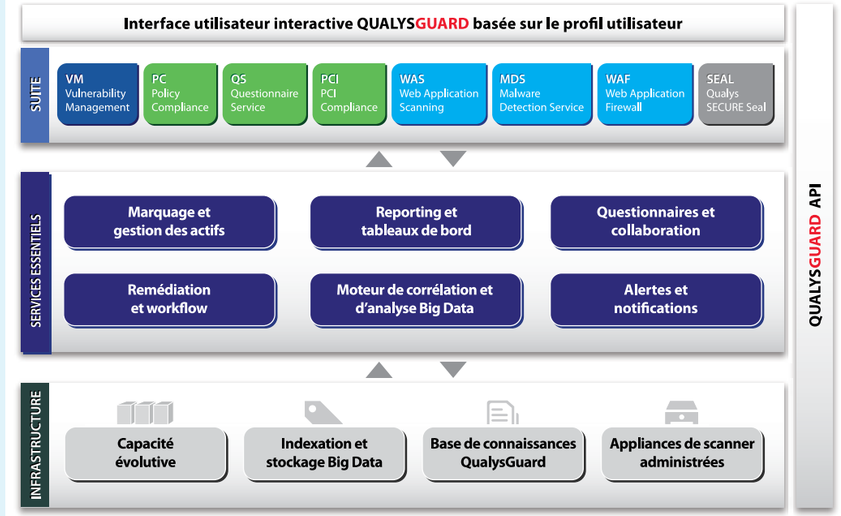
Indexation et stockage des données volumineuses (Big Data)
Reposant sur notre modèle de stockage de données sécurisé, le moteur d'analyse de QualysGuard indexe des péta-octets de données et utilise ces informations en temps réel afin d'exécuter des tags ou des règles pour mettre à jour dynamiquement les propriétés d'actifs informatiques qui sont utilisées dans différents processus d'analyse, de reporting et de remédiation.

Base de connaissances
QualysGuard se fonde sur la base de connaissances QualysGuard, notre référentiel exhaustif des vulnérabilités connues et des contrôles de conformité pour un grand nombre d'équipements, de technologies et d'applications qui est au cœur de notre technologie de sécurité et de conformité. Cette base de connaissances est mise à jour de manière dynamique et permanente à l'aide d'informations sur les nouvelles vulnérabilités, de vérifications de contrôle, de correctifs validés et d'améliorations du contenu.

Appliances administrées
Qualys héberge et administre des milliers d'appliances physiques réparties à travers le monde et qui servent à évaluer les systèmes externes et les applications Web des entreprises. Pour évaluer leurs actifs informatiques internes, les entreprises déploient des appliances physiques ou des images virtuelles téléchargeables au sein de leur réseau interne. Les appliances QualysGuard se mettent à jour de manière transparente à l'aide de notre technologie de gestion automatisée et propriétaire.

Services de base QualysGuard

Les services de base QualysGuard fournissent des workflows intégrés, une gestion ainsi qu'une analyse et un reporting en temps réel sur l'ensemble de nos solutions de gestion de la sécurité informatique et de la conformité. Nos services de base comprennent :



Marquage et gestion des actifs
Grâce à cette technologie, les entreprises peuvent identifier, classer et gérer facilement de gros volumes d'actifs dans des environnements informatiques hautement dynamiques. Elles peuvent également automatiser le processus de gestion de l'inventaire et l'organisation hiérarchique des actifs informatiques.

Reporting et tableaux de bord
Un moteur de reporting hautement configurable vous fournit des rapports et des tableaux de bord basés sur le profil des utilisateurs et les privilèges d'accès.

Questionnaires et collaboration
Un questionnaire configurable vous permet de capturer facilement les processus métier et les workflows existants afin d'évaluer les contrôles et de collecter des éléments de preuves pour valider et documenter la conformité.

Remédiation et workflow
Avec un moteur de workflow intégré, votre entreprise peut générer automatiquement des tickets de remédiation destinés au Help Desk et gérer les exceptions de conformité à partir de politiques organisationnelles, ce qui permet de fournir ultérieurement des analyses, des commentaires, du suivi et une remontée d'informations. Ce moteur distribue automatiquement les tâches de remédiation aux administrateurs informatiques après exécution de l'analyse. De plus, il assure un suivi des progrès de remédiation et ferme les tickets ouverts une fois les correctifs appliqués et la remédiation vérifiée lors d'analyses ultérieures.

Moteur de corrélation et d'analyse des données volumineuses
Un moteur d'analyse indexe, recherche et assure la corrélation de péta-octets de données de sécurité et de conformité avec d'autres incidents de sécurité et des informations de sécurité provenant de tiers. Des workflows intégrés vous permettent d'évaluer rapidement le risque et de consulter des informations de remédiation, des analyses d'incidents et des travaux de recherche.

Alertes et notifications
Un moteur d'alerte crée des notifications par courriel pour alerter les membres de l'équipe sur les nouvelles vulnérabilités, les infections à base de codes malveillants, les analyses réalisées, les tickets de panne ouverts ainsi que les mises à jour système.

Suite QualysGuard dans le Cloud

Avec QualysGuard, votre entreprise peut utiliser les solutions dont elle a besoin, quand elle en a besoin et payer uniquement ce dont elle se sert. Votre entreprise peut s'abonner à une ou plusieurs de nos solutions de sécurité et de conformité et utiliser davantage de produits au fur et à mesure de ses besoins.

Vulnerability Management
QualysGuard VM est une solution de pointe et primée qui automatise l'audit du réseau et la gestion des vulnérabilités à travers l'entreprise. Cette offre procède notamment à la découverte et à la cartographie du réseau, à la gestion des actifs ainsi qu'au reporting des vulnérabilités et au suivi de la remédiation. S'appuyant sur notre base de connaissances exhaustive des vulnérabilités connues, QualysGuard VM offre une protection efficace contre les vulnérabilités, le tout sans déployer d'énormes ressources.

Policy Compliance
Grâce à QualysGuard PC, les entreprises peuvent analyser et collecter des informations de configuration et de contrôle d'accès auprès d'équipements en réseau et d'applications Web. Ensuite, cette solution procède automatiquement au mappage de ces informations avec les politiques internes et la réglementation en vigueur pour documenter la conformité. Totalement automatisée, QualysGuard PC réduit le coût de la conformité pour les entreprises, le tout sans recourir à des agents logiciels.

Questionnaire Service
QualysGuard QS est une solution dans le Cloud qui centralise et automatise le lancement, le suivi, l'analyse et l'approbation des évaluations relatives aux risques et à la conformité. Ce service de questionnaires réduit le coût et les efforts de collecte des informations auprès des différentes parties prenantes. Il aide aussi les entreprises à rationaliser et à étendre leurs programmes de gestion des risques fournisseurs et informatiques et d'évaluation de leur conformité.

PCI Compliance
QualysGuard PCI peut fournir aux entreprises qui stockent des données sur les détenteurs de cartes une solution rentable et hautement automatisée qui vérifie et renseigne sur la conformité à la norme PCI DSS. Avec QualysGuard PCI, les commerçants peuvent remplir le questionnaire d'auto-évaluation PCI annuel et exécuter des analyses de vulnérabilités pour réaliser les audits PCI trimestriels et garantir la sécurité des applications Web.

Web Application Scanning
Service d'analyse des applications Web, QualysGuard WAS s'appuie sur l'évolutivité de notre plate-forme Cloud pour donner aux entreprises les moyens de découvrir, de cataloguer et d'analyser toutes les applications Web de l'entreprise. QualysGuard WAS parcourt et analyse les applications Web personnalisées et identifie les vulnérabilités qui menacent les bases de données sous-jacentes ou qui contournent les contrôles d'accès aux applications.

Malware Detection Service
Avec le service de détection des codes malveillants QualysGuard MDS, les entreprises sont en mesure d'analyser, d'identifier et de supprimer les infections à base de codes malveillants de leurs sites Web. QualysGuard MDS s'appuie sur une analyse comportementale et statique qui détecte les codes malveillants et surveille en permanence les sites Web.

Web Application Firewall
QualysGuard WAF est un pare-feu pour applications Web qui assure la sécurité des applications Web d'entreprise sans les coûts, ni l'encombrement ni la complexité liés aux solutions de pare-feu pour applications Web qui reposent sur une appliance. Cette solution protège les applications Web contre les vecteurs d'attaque en améliorant les configurations par défaut de ces applications Web ainsi que les correctifs virtuels.

QualysGuard WAF accroît aussi les performances des sites Web en réduisant les temps de chargement des pages, en optimisant la bande passante et en s'appuyant sur notre réseau mondial de caches Web.

Qualys SECURE Seal
Avec QualysGuard SECURE Seal, les entreprises peuvent prouver à leurs clients en ligne qu'elles adoptent un programme de sécurité proactive. Analysant notamment la présence de codes malveillants et de vulnérabilités au sein des applications Web et sur le réseau, le sceau de confiance SECURE Seal valide aussi l'intégrité des certificats SSL. Les entreprises sans problème de sécurité critique peuvent afficher un sceau QualysGuard SECURE sur leurs sites Web.

Pourquoi Qualys ?

La vision de Qualys consiste à transformer la manière dont les entreprises sécurisent et protègent leurs infrastructures informatiques et leurs applications. Qualys est le meilleur choix pour tous vos besoins de sécurité et de conformité.

Une marque de confiance pour la sécurité dans le Cloud

Pionnier de la sécurité dans le Cloud et fournisseur de confiance et réputé pour ses évaluations des vulnérabilités et de la conformité à la fois fiables et précises, Qualys a lancé la première solution de gestion des vulnérabilités en tant que service dès 2000.

Une plate-forme de sécurité dans le Cloud évolutive et extensible

Grâce à notre architecture Cloud hautement évolutive et à nos solutions de gestion de la sécurité et de la conformité modulaires, des entreprises de toute taille et présentes sur de nombreux marchés s'appuient sur nos ressources pour garantir la sécurité de leur infrastructure. Notre plate-forme Cloud est utilisée aussi bien par des petites entreprises que par des grands comptes implantés dans le monde entier qui possèdent des millions d'équipements et d'applications en réseau.

Un long historique d'innovation pour la sécurité et la conformité dans le Cloud

Depuis plus de 12 ans, Qualys propose des solutions novatrices de sécurité et de conformité dans le Cloud pour que nos clients puissent protéger leur environnement informatique plus efficacement et à moindre coût. Nous avons considérablement investi dans la plate-forme dans le Cloud QualysGuard et nous sommes particulièrement bien positionnés pour relever les défis d'un paysage de la sécurité et de la conformité informatique qui évolue en permanence.

Payez pour ce que vous utilisez et lorsque vous vous en servez

Nos clients utilisent une ou plusieurs solutions QualysGuard sans risque et depuis n'importe quel navigateur Web. Grâce à ce modèle, ils peuvent s'abonner aux seules solutions dont ils ont vraiment besoin, sachant qu'ils pourront étendre et amplifier facilement leur déploiement en fonction de l'évolution de leurs besoins.

Pour nous demander une version d'évaluation gratuite de la Suite QualysGuard dans le Cloud, rendez-vous à l'adresse www.qualys.com/trials/fr

50+ des Forbes Global 100

ont adoptè la plate-forme de sècuritè et de conformitè dans le Cloud QualysGuard

8 des 10 premières entreprises **Logiciels**

8 des 10 premières entreprises **Biotechnologies**

8 des 10 premières entreprises **Matériel technologique**

8 des 10 premières entreprises **Distribution**

7 des 10 premières entreprises **Matériel Médical**

7 des 10 premières entreprises **Banque**

7 des 10 premières entreprises **Médias**

7 des 10 premières entreprises **Distribution alimentaire**

6 des 10 premières entreprises **Construction automobile**

6 des 10 premières entreprises **Chimie**

6 des 10 premières entreprises **Télécoms**

6 des 10 premiers **Conglomérats**

QUALYS®
CONTINUOUS SECURITY

Qualys Technologies
Maison de la Défense
7 Place de la Défense
92400 Courbevoie, France
T: +33 (0) 1 41 97 35 70, info-fr@qualys.com

Qualys est une société d'envergure mondiale avec des représentations dans le monde entier. Pour connaître le bureau le plus proche de chez vous, rendez-vous sur **http://www.qualys.com**