PRÉSENTATION DE SOLUTION

Sécurité du cloud : garantir le maintien de la conformité

État des lieux
Si les systèmes A et B (approuvés) sont 100 % conformes à un instant t, mais que le système C (non approuvé) qui sert de réplica de base de données pour A et B n'a aucune existence officielle, difficile de valider la conformité des systèmes A et B.

Si le système D (approuvé) est complètement conforme à ce jour, mais qu'il n'existe aucune preuve de sa conformité entre le dernier audit et aujourd'hui, impossible de prouver le maintien de sa conformité pendant ce laps de temps.

De nombreux types d'audits de conformité exigent des preuves suivies (récurrentes ou continues) de due diligence dans le cadre du processus de certification.

Pour pouvoir être maintenue en continu et à grande échelle, cette due diligence doit être automatisée au maximum afin de réduire – et non d'augmenter – les coûts d'exploitation.

Compliance assurance : garantir le maintien de la conformité
La compliance assurance consiste à établir des preuves formelles que toutes les mesures nécessaires et raisonnables ont été prises (ce que l'on appelle la due diligence) afin de dédouaner un professionnel, un groupe ou une organisation d'un certain nombre de responsabilités (juridiques ou autres). Les coûts liés à de telles activités se justifient tant qu'ils permettent d'établir la due diligence. Les budgets de sécurité sont souvent alloués en conséquence.

Mais si la compliance assurance doit faire figure de priorité dans ces budgets, elle doit aussi s'inscrire au cœur de toute solution de lutte contre les menaces de sécurité persistantes et avancées. Même si une entreprise ne peut neutraliser toutes les menaces avancées à l'aide de simples contrôles de conformité, elle peut filtrer le gros des interférences en validant constamment la conformité de nombreux éléments de base.

Automatiser la compliance assurance reste encore le meilleur moyen de veiller à l'efficacité et à l'exhaustivité de ces activités. Aujourd'hui, les entreprises ont besoin d'une solution réellement utile et économique, couvrant un ensemble plus vaste de ressources et capable de vérifier leur conformité à plusieurs niveaux. Parmi les éléments à contrôler doivent figurer les configurations et correctifs des applications cloud (comme les fonctions sans serveur), des réseaux (les VPN, par exemple), des services et des workloads, ainsi que ceux des systèmes d'exploitation traditionnels.

Problèmes fondamentaux
Au cours de leurs missions de maintien de la conformité de leurs environnements de cloud public et privé, les équipes de sécurité rencontrent de nombreux obstacles. C'est d'autant plus vrai lorsque leurs différents types de ressources cloud s'étendent à de multiples comptes et fournisseurs cloud, systèmes d'exploitation, régions, services et autres groupes logiques.

Sans visibilité complète et automatisée sur l'état de leurs ressources et l'historique de conformité de leurs environnements multicloud, les entreprises perdent un temps précieux à chaque audit. Pour de nombreux collaborateurs, la compliance assurance devient cet énorme fardeau qui n'apporte visiblement rien de bon, sans parler des coûts d'exploitation énormes qu'elle engendre.

Les entreprises peinent à intégrer leurs activités de conformité à leurs outils et processus d'automatisation existants. De fait, il leur est difficile d'améliorer l'efficacité de ces activités à l'aide du modèle DevOps.

De même, elles ont du mal à trouver des solutions techniques utiles aux problèmes courants de la compliance assurance, en grande partie à cause du manque de fonctionnalités critiques nécessaires sur les outils de conformité traditionnels. Parmi celles-ci :

- Inventaire automatique et complet des ressources via les API des fournisseurs cloud
- Application intégrée de vérifications de conformité via l'élimination inline des risques
- Visibilité complète sur les vulnérabilités aux niveaux du cloud et de l'OS
- Réponses orientées événements (alertes, rapports, remédiation, etc.) aux violations de conformité détectées
- Prise en charge des exceptions temporelles aux règles de conformité en fonction des besoins métiers
- Configuration groupée des paramètres de conformité pour les sous-ensembles de ressources détectées
- Analyses de conformité à la demande (orientée API) de la ou des ressources indiquées
- Analyse du risque pour permettre aux équipes de trier les tâches de remédiation
- Gestion en standard des principales normes courantes de reporting de conformité

Critères de la solution idéale

Les environnements cloud sont dynamiques par nature. Si les utilisateurs du cloud peuvent créer les ressources dont ils ont besoin à tout moment, cela signifie aussi que ces ressources peuvent être modifiées, voire supprimées n'importe quand.

À l'aide d'identifiants de compte cloud compromis, des attaquants peuvent obtenir un accès illimité à des ressources non autorisées et non sécurisées, hors du contrôle des outils de surveillance traditionnels. Pour établir des preuves (suivies) de due diligence pour toutes les ressources d'infrastructure concernées – à des fins de compliance assurance – les solutions de sécurité du cloud doivent à la fois :

- Tenir continuellement l'inventaire complet de ces ressources, y compris un registre détaillé de l'état de chacune avec fonction de recherche
- Conserver l'historique complet des événements de sécurité de chaque ressource, y compris les résultats des contrôles de conformité créés par la solution

Dans l'idéal, une seule solution doit pouvoir évaluer la conformité à travers de nombreux périmètres d'infrastructure logique et physique. Ainsi, les utilisateurs peuvent utiliser des requêtes ad hoc et prédéfinies pour agréger les risques (écarts de conformité) par attribut logique, tandis que les équipes DevOps et SecOps peuvent prioriser les activités de remédiation en fonction des zones vulnérables.

À partir des données des API des fournisseurs cloud, cette solution de compliance assurance doit produire un ensemble de données contextualisées que les utilisateurs peuvent interroger et filtrer via une interface graphique ou une API pour créer de nouveaux contrôles de conformité sur-mesure. Elle doit être aussi puissante que simple d'utilisation pour les audits de base sur l'inventaire des ressources, la lecture des résultats des contrôles de conformité et la production des rapports de compliance assurance. Suffisamment flexible, le moteur de conformité de cette solution doit pouvoir gérer des formes atypiques et avancées de contrôles de conformité afin de répondre aux besoins uniques de votre entreprise.

GARANTIE DU MAINTIEN DE LA CONFORMITÉ : LES CRITÈRES DE SÉLECTION

- **Étendue**
  Capacité à exécuter un large éventail de contrôles de conformité à différents niveaux du parc technologique actuel, sur les comptes et services cloud, les identités (utilisateurs, groupes, rôles), les réseaux, les systèmes d'exploitation, les correctifs, etc.

- **Profondeur**
  Capacité à collecter des données contextuelles approfondies sur la configuration et les comportements des ressources. La plupart des produits de sécurité privilégient l'étendue du champ d'action aux dépens de la profondeur contextuelle, ou inversement. La solution idéale approfondit les contrôles de conformité à travers de multiples couches (niveaux) du parc technologique.

- **Intégration**
  Capacité à fonctionner en conjonction avec les outils opérationnels existants. À l'heure où la détection précoce des écarts de conformité devient un véritable enjeu, il est plus important que jamais d'intégrer les contrôles de conformité automatisés aux pipelines de déploiement DevOps (CI/CD). Votre solution doit fournir une API RESTful pour l'intégration à la demande des fonctions de conformité aux environnements de tests Agile. Ainsi, les équipes de déploiement pourront détecter et corriger les failles dans les premiers environnements de tests (« Dev », « Lab », « QA », etc.).

La solution Cloudvisory
La solution Cloudvisory garantit le maintien de la conformité des environnements multicompte, multicloud et multi-système d'exploitation. Ses fonctionnalités de conformité détectent automatiquement les risques par le biais de vérifications configurables des ressources, contrôles et événements connus, tout en offrant un certain nombre de réponses manuelles et automatisées possibles (alertes, rapports, remédiation). Cloudvisory intègre plus de 1 300 contrôles de conformité et facilite la personnalisation des points de vérification existants et la création de nouveaux.

Par ailleurs, une interface utilisateur du type « point-and-click » simplifie et accélère la création de vérifications de conformité continues (à savoir des contrôles de conformité réguliers dont la fréquence est configurable) à partir de résultats d'audits ad hoc. La solution retrace l'historique complet des contrôles de conformité associés aux ressources cloud inventoriées et intègre des fonctionnalités enrichies de reporting qui permettent de respecter vos obligations internes et externes de compliance assurance. Elle génère et exporte facilement des rapports de conformité dans différents formats (PDF, XLS, CSV, etc.) pour toutes vos vérifications et n'importe quel sous-ensemble de points de contrôle (pour des rapports de conformité ou standards internes sur mesure). Enfin, elle fournit des rapports intégrés sur les normes de conformité prises en charge.

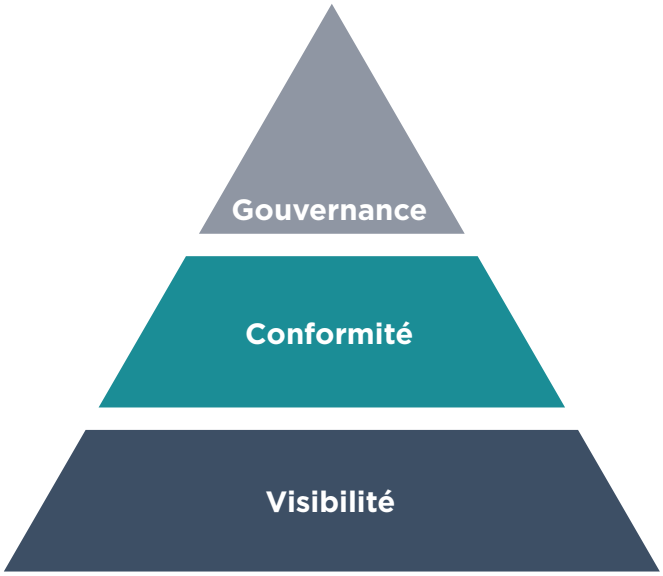
Pourquoi Cloudvisory
Seule Cloudvisory offre aux entreprises une solution de compliance assurance aussi complète. Sur les produits concurrents, il manque toujours une ou plusieurs fonctionnalités indispensables :

- Prise en charge étendue de multiples fournisseurs cloud et systèmes d'exploitation
- Couverture étendue pour parvenir à une due diligence suffisante sur une couche de conformité donnée (cloud, système d'exploitation)
- API RESTful nécessaires pour intégrer l'automatisation des opérations de conformité aux outils et processus opérationnels existants

Cloudvisory offre une visibilité complète et, par là même, un contexte suffisant pour évaluer les différents niveaux et états de conformité d'une ressource donnée. Elle intègre des fonctionnalités essentielles comme la remédiation inline configurable, le traitement temporel des exceptions approuvées aux règles de conformité, l'analyse de conformité à la demande de ressources données via les API Cloudvisory, mais aussi les agrégations de risques avec accès aux détails qui permettent aux analystes sécurité d'évaluer les risques à travers différents périmètres d'infrastructure physique et logique.

Les produits concurrents tendent à offrir des solutions de conformité limitées (axées sur un seul fournisseur cloud ou système d'exploitation) et basées sur un champ de vision restreint (fichiers journaux uniquement). C'est pourquoi ils affichent des résultats irréguliers et contribuent peu à l'efficacité des pratiques de compliance assurance d'une entreprise. Cloudvisory se démarque par un socle robuste de fonctionnalités d'entreprise alliées à un cadre de conformité leader et extensible. Elle facilite l'automatisation des activités de maintien de la conformité dans n'importe quel environnement. En somme, elle aide les entreprises à renforcer leur sécurité tout en réduisant leurs coûts.

L'union fait la force
Le volet conformité de Cloudvisory s'appuie sur le contexte détaillé fourni par les fonctionnalités de visibilité de notre solution. En plus de s'adapter à tous vos objectifs de conformité, il permet de créer facilement de nombreux contrôles de base personnalisés, à partir de requêtes ad hoc sur les ensembles de données de visibilité que seul Cloudvisory peut fournir. Ces ensembles de données distincts comprennent les configurations de ressources cloud (des VM, par exemple), celles des contrôles de sécurité cloud (politiques IAM, groupes de sécurité réseau, etc.) ; les journaux d'objets cloud, ceux des flux réseau, les configurations des systèmes d'exploitation et leurs journaux. Vous pouvez aisément créer des ensembles de contrôles de conformité sur-mesure pour répondre à vos propres besoins de garantie de conformité.



Normes et réglementations couvertes

Fournisseurs cloud

- CIS Benchmark pour AWS
- RGPD sur AWS
- HIPAA sur AWS
- NIST 800-53 Revision 4 sur AWS
- PCI DSS 3.2 sur AWS
- CIS Benchmark pour Azure
- RGPD sur Azure
- HIPAA sur Azure
- NIST 800-53 Revision 4 sur Azure
- PCI DSS 3.2 sur Azure
- CIS Benchmark pour Kubernetes
- Check-list de sécurité OpenStack

Systèmes d'exploitation

- CIS Benchmark pour CentOS
- CIS Benchmark pour Red Hat
- CIS Benchmark pour Ubuntu 16.04
- CIS Benchmark pour Ubuntu 18.04

Clouds publics

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

Gartner Cool Vendor 2018

Cloudvisory élu Gartner Cool Vendor dans la catégorie Sécurité cloud 2018.

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS-2017

Cloudvisory classé par CIO Applications dans le top 25 des fournisseurs de solutions Amazon.

AICPA SOC

Cloudvisory : SaaS certifié SOC 2 par un audit indépendant.

Pour en savoir plus sur FireEye, rendez-vous sur : **www.FireEye.com/cloudvisory**

FireEye, France
Nextdoor Cœur Défense
110 Esplanade du Général de Gaulle
92931 Paris La Défense Cedex 92974
+33 1 70 61 27 26
france@FireEye.com | www.FireEye.fr
FireEye, Inc.
601 McCarthy Blvd.
Milpitas, CA 95035
+1 408 321 6300 | info@FireEye.com

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Threat Intelligence. Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.

FIREEYE™