PRÉSENTATION DE SOLUTION

Sécurité du cloud : la fin des angles morts

D'après une vaste étude, 43 % des 400 000 personnes interrogées considèrent la « visibilité sur la sécurité de l'infrastructure » comme un problème majeur.

Rapport sur la sécurité dans le cloud
Cybersecurity Insiders

État des lieux
Tôt ou tard, la majorité des entreprises sont victimes d'un piratage, souvent à leur insu.

Et dans les rares cas où la compromission est détectée, elle l'est le plus souvent après six à douze mois, découverte par hasard ou par un acteur extérieur (client ou chercheur en sécurité, par exemple).

De fait, une entreprise a plus de chances d'être avisée d'une compromission de données par un acteur extérieur bienveillant que par ses équipes opérationnelles internes.

Sachant que ces statistiques proviennent d'entreprises « en conformité » au moment de l'incident, que dire de celles peu versées dans les questions de conformité ou d'investigations post-violation.

En tout état de cause, mieux vaut découvrir une compromission soi-même et à un stade précoce que d'en être informé par ses clients.

Déficit de visibilité
La visibilité est la clé de voûte de n'importe quelle stratégie de sécurité dans le cloud, ce quelles qu'en soient les priorités : conformité, traque des menaces, application des politiques ou atténuation des risques.

Le problème, c'est que cette visibilité reste un vœu pieux dans nombre d'entreprises. Enquête après enquête, les professionnels de la cybersécurité nous révèlent ainsi que leur problème n°1 reste le manque de visibilité sur la sécurité de leur infrastructure.

D'où l'importance de régler ce problème en priorité avant de nourrir une stratégie de sécurité plus ambitieuse.

Problèmes fondamentaux
De nombreux obstacles se dressent sur la voie des équipes de sécurité cherchant à établir une vue centralisée et contextualisée de leur environnement SecOps, condition sine qua non à la traque des mouvements latéraux des attaquants infiltrés.

Et ce déficit de visibilité ne fait que se creuser à mesure que les entreprises se développent et que leurs équipes, processus et technologies de déploiement se diversifient, pour finalement aboutir à une nébuleuse opaque de fournisseurs, comptes, régions et services cloud.

Si les déploiements en self-service ont rendu les entreprises plus efficaces, cette flexibilisation s'est opérée au détriment de la capacité à centraliser le provisionnement et la surveillance d'une infrastructure à sécurité renforcée. À des degrés divers, les technologies cloud ont favorisé des déploiements d'infrastructure plus étendus, plus distribués, dynamiques par nature et (parfois) éphémères. Mais pendant ce temps, les outils de sécurité traditionnels n'ont su ni tenir le rythme, ni se hisser à l'échelle du cloud. Ces dix dernières années, les technologies d'automatisation des déploiements ont également pris de vitesse les technologies d'automatisation de la sécurité sur des critères essentiels tels que l'adoption, les fonctionnalités et la maturité.

Par le passé, les opérations de sécurité étaient axées sur la prévention plutôt que la détection. Mais nulle prévention n'est infaillible. De même, la prévention traditionnelle reposait sur des contrôles statiques concentrés sur le périmètre de l'entreprise. Or, dans le cloud, le périmètre est par nature dynamique plutôt que statique, et défini au niveau logique plutôt que physique.

Les outils de sécurité d'ancienne génération, à l'image des pare-feu physiques et virtuels, ne sont pas conçus pour repousser et détecter des attaques dans des environnements cloud distribués et dynamiques. D'autant que le rythme rapide des changements dans le cloud, conjugué à des déploiements de plus en plus distribués et hétérogènes, complique la donne côté visibilité. Difficile de trouver une solution de sécurité capable de répondre à tous ces enjeux.

Critères de la solution idéale
Pour éclairer les nombreuses zones d'ombre, la solution doit assurer une surveillance étendue et approfondie des configurations présentes et des événements de sécurité passés pour chaque ressource.

Mais qui dit visibilité complète sur la sécurité de l'infrastructure dit conjonction de plusieurs faisceaux :

- **Inventaire complet de toutes les ressources concernées à tout instant**
  En l'absence de visibilité (présente et passée) sur la totalité des ressources de l'environnement, les audits de conformité produiront des résultats incomplets et/ou trompeurs.
- **Possibilités de recherche d'informations contextuelles sur l'état des ressources individuelles à un instant t**
  Sans visibilité sur l'état actuel de toutes les ressources concernées, impossible de produire le moindre contexte. Et sans contexte, les concepts d'assurance conformité et de détection des anomalies perdent tout leur sens.
- **Historique complet des événements de sécurité concernés pour chaque ressource**
  En l'absence de visibilité sur le comportement réel des workloads et des utilisateurs, il est impossible de s'assurer de l'efficacité des contrôles et de l'absence d'intrus au sein même de l'environnement.

Les simples déductions à partir des logs (ou journaux) ne suffisent pas. Certaines données font encore défaut à l'issue de périodes de mise en route, interruptions de service et autres types de défaillance.

Si l'état de configuration actuel de chaque ressource n'est pas directement connu à partir des API respectifs du fournisseur cloud, l'inventaire des ressources reste incomplet. Dès lors, des attaquants peuvent facilement se soustraire à la détection. Les journaux contiennent certes des informations utiles, mais les API ne mentent pas.

Une solution efficace doit donc offrir une visibilité complète sur des déploiements complexes et distribués, y compris les environnements cloud hybrides et multi-cloud, qui peuvent être gigantesques, éphémères ou sans serveur. La solution nécessite donc une visibilité complète, mais elle doit aussi offrir une vue consolidée et interrogeable de toutes les formes de contexte disponibles pour chaque ressource. La solution de visibilité doit permettre aux utilisateurs d'exécuter des requêtes spécifiques, par interface native ou API, sur le contexte enregistré de chacune des ressources concernées. Le tout sous une même interface pour pouvoir effectuer des analyses de sécurité et des audits de conformité sur tous les clouds.

La solution idéale doit faciliter la conversion des requêtes d'audit ponctuelles en contrôles de conformité récurrents, non seulement pour éclairer les zones d'ombre, mais aussi pour faire de cette visibilité la base de pratiques de sécurité plus évoluées (assurance conformité, application des politiques, traque des menaces, etc.).

CLOUDVISORY, VOTRE ASSURANCE VISIBILITÉ

À elle seule, la solution Cloudvisory fournit une visibilité complète sur la sécurité de n'importe quelle infrastructure. La détection des ressources est totalement automatisée, et Cloudvisory gère la totalité des ressources concernées en temps réel. La détection automatique par les API du fournisseur cloud apporte un contexte approfondi, dans la mesure où Cloudvisory stocke les détails du dernier état connu de chaque ressource ayant existé dans un environnement sous gestion. L'état de chaque ressource se compose ainsi de plusieurs niveaux d'information :

- **Contexte cloud :** détails sur le fournisseur cloud/compte/région/groupe/rôle/etc. associé à chaque ressource.
- **Contexte historique :** analyses déduites de l'historique des enregistrements d'événements de sécurité créés tout au long du cycle de vie d'une ressource
- **Contexte de sécurité :** configurations de l'état actuel des contrôles de sécurité d'une ressource
- **Contexte système :** informations sur l'état présent de la ressources, obtenues directement de son système d'exploitation

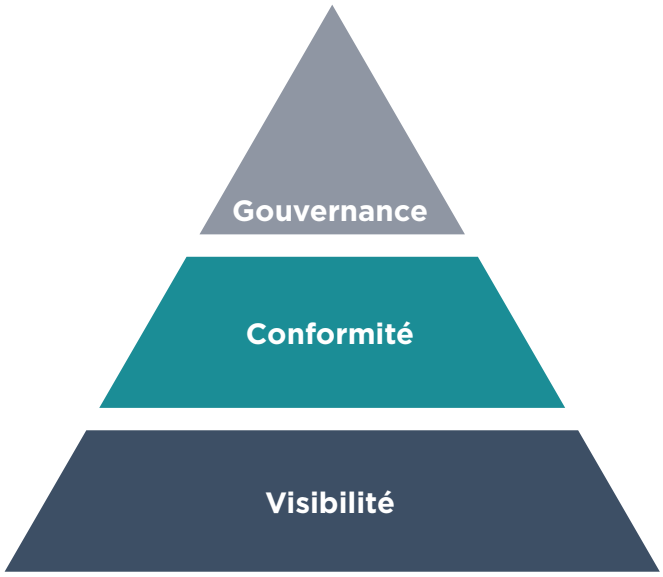
Pourquoi Cloudvisory

La solution Cloudvisory fournit la meilleure couverture pour tous vos environnements multi-cloud et multi-systèmes d'exploitation, mais pas seulement. Cloudvisory a aussi été conçue pour assurer une parfaite interopérabilité du triptyque visibilité, conformité et gouvernance.

De nombreux produits peuvent évaluer rapidement votre niveau de sécurité sur plusieurs déploiements et comptes d'un même fournisseur cloud. Le problème, c'est que la majorité des entreprises ont adopté une stratégie de cloud hybride ou multi-cloud, ce qui limite sérieusement leur options côté sécurité. Cloudvisory est la seule solution de sécurité multi-cloud offrant une rentabilité immédiate (grâce à une visibilité complète), tout en servant de base à l'amélioration de la sécurité sur le long terme.

L'union fait la force

Qui dit conformité dit visibilité. Et en même temps, la récurrence des contrôles de conformité génère de la visibilité. Le cercle vertueux est donc enclenché. Cette relation synergique produit un contexte sécuritaire et historique servant à alimenter des algorithmes de machine learning qui traduiront ces données en politiques intelligentes du moindre privilège, gage d'une gouvernance renforcée de la sécurité.



Clouds publics couverts

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

Systèmes d'exploitation pris en charge

- CentOS
- Redhat
- Ubuntu Linux

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 Cloudvisory, rendez-vous sur **www.FireEye.com/cloud**

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™