FIREEYE™

LIVRE BLANC

Micro-segmentation et orchestration de la sécurité pour une défense du cloud à toute épreuve

Sommaire

Le cloud est assiégé de toutes parts

Des PME aux multinationales, les entreprises de toutes tailles sont en pleine migration de leurs environnements informatiques vers des clouds publics et privés. Recentrage sur le client, agilité opérationnelle et réduction des coûts : tels sont les moteurs de ce grand chantier infrastructurel. Mais les data centers et les architectures cloud n'échappent pas pour autant aux menaces, tout comme leurs équivalents « on-premise ». Les uns comme les autres sont vulnérables aux mouvements latéraux des attaquants.

Quelles solutions ?

Visibilité et configuration des contrôles

Pour limiter l'impact potentiel des menaces, votre organisation doit pouvoir identifier et neutraliser rapidement tout risque de malware. Mais encore faut-il pouvoir disposer d'une visibilité fiable et cohérente sur tous les aspects de votre environnement. Pour le cloud, cela peut s'avérer difficile, dans la mesure où 37 % des sondés d'une récente enquête avouent que « le manque de visibilité sur la sécurité de leur infrastructure représente leur plus gros casse-tête relatif au cloud ».

Quant aux équipements du périmètre réseau et aux politiques de sécurité réseau traditionnelles, ils sont peu adaptés aux environnements cloud. Au-delà du pare-feu, les équipes de sécurité n'ont que peu de moyens pour arrêter les attaques.

Les principaux fournisseurs cloud proposent tous des contrôles intégrés qui permettent d'appliquer les politiques de sécurité avant que le trafic n'atteigne les workloads. À l'inverse, les défenses périmétriques basées sur le système d'exploitation restent cantonnées à l'intérieur de la zone d'attaque, ce qui accroît les risques puisque les décisions de sécurité ne sont prises que lorsque le flux de données a atteint la machine virtuelle. Conçus sur une approche granulaire reposant sur des listes blanches au niveau des workloads, les contrôles cloud-native doivent être explicitement configurés avant que les données puissent entrer ou sortir d'un workload, d'une instance ou d'un container. Les configurations avec contrôles d'accès basés sur le principe du moindre privilège sont essentielles pour une sécurité vraiment efficace.

Erreurs de configuration et mauvaise gestion des contrôles de sécurité

En matière de contrôles de sécurité cloud-native, il est important de bien comprendre qui fait quoi et comment. Il se peut qu'au départ, les équipes DevOps des fournisseurs cloud codent les contrôles de sécurité dans leurs scripts d'orchestration, mais se pose alors la question de l'évolutivité :

- Les équipes de sécurité peuvent n'avoir aucune visibilité et donc aucune compréhension des contrôles déployés, même avec la console du fournisseur cloud.
- Les équipes DevOps peuvent utiliser des paramètres génériques pour des contrôles complexes, aboutissant à un accès trop permissif et un risque accru pour l'entreprise.

« Vu la capacité des menaces avancées à contourner le périmètre traditionnel et les systèmes de protection basés sur les signatures, les contrôles de sécurité doivent devenir automatisables et adaptatifs. »

Source : Gartner

CONTRÔLES DE SÉCURITÉ CLOUD-NATIVE :
« La position de Gartner sur la sécurité du cloud est claire : les services de cloud public proposés par les principaux fournisseurs de cloud sont sûrs. Utilisez les contrôles de sécurité cloud-native des fournisseurs IaaS. »

« L'exploitation de ces contrôles nous a permis de passer d'un réseau sécurisé de workloads à un réseau de workloads sécurisés. »

— Vice-président senior de l'infrastructure.

« En 2020, 80 % des violations de sécurité dans le cloud seront dues à des erreurs de configuration et de gestion, et non à des vulnérabilités inhérentes aux fournisseurs. »

Source : Gartner

- Même si le cloud est un environnement explicitement placé sur liste blanche, les paramètres configurés par les équipes DevOps donnent parfois un accès insuffisant.
- Comme elles disposent d'une gestion et d'un contrôle limités sur les paramètres de sécurité, les équipes DevOps doivent en permanence s'impliquer dans les mises à jour à mesure que les workloads montent en charge.
- Cela ralentit les opérations de développement et de déploiement car elles ne disposent pas d'un moyen simple pour ajuster les politiques existantes sur de multiples applications sans codage ni script complexes.

Planifier un environnement cloud élastique et dynamique

Étant donné les mouvements et les changements perpétuels des workloads, les politiques de sécurité peuvent vite devenir inopérantes et inefficaces dans n'importe quel environnement cloud.

Pour s'adapter à ce changement permanent, les équipes DevOps peuvent tenter d'assimiler les contrôles des différents fournisseurs et d'écrire des scripts, mais cela peut occasionner des retards de déploiement, augmenter le risque et créer des problèmes d'audit en interne.

Un plan de sécurité renforcée doit s'appuyer sur ces différents piliers :

- **Visibilité étendue :** Visualisation de l'ensemble de infrastructure et de ses contrôles de sécurité pour rapidement identifier les risques environnementaux et confirmer le déploiement d'une politique adaptée.
- **Orchestration et automatisation de la sécurité :** Provisionnement et déprovisionnement automatiques de contrôles spécifiques pour réduire les risques d'erreur de configuration et accélérer les opérations.
- **Micro-Segmentation :** Modèle automatique pour appliquer des règles granulaires et précises sur les machines virtuelles et les containers, basées sur la fonction du workload.
- **Surveillance et gouvernance :** Mécanisme de suivi de l'état de sécurité et d'identification des risques et des menaces potentiels.
- **Acheter vs. développer en interne :** Solution fiable et « off-the-shelf » pour répondre à toutes vos exigences.

L'approche moderne de la sécurité du cloud

Dans son livre blanc de 2016 intitulé « Comment rendre les workloads IaaS plus sécurisés que dans votre propre data center », Gartner suggérait les étapes suivantes:

1. Utilisez les contrôles de sécurité cloud-native du fournisseur IaaS ainsi que les pratiques DevOps et d'automatisation.
2. Micro-segmentez par défaut : Passez d'un « réseau sécurisé de workloads » à un « réseau de workloads sécurisés. »
3. Des niveaux élevés d'automatisation réduisent considérablement les erreurs de gestion et de configuration, ce qui limite la surface d'attaque — et améliore grandement la sécurité.
4. Journalisez tout et exigez une visibilité constante — on ne peut pas protéger ce que l'on ne voit pas.

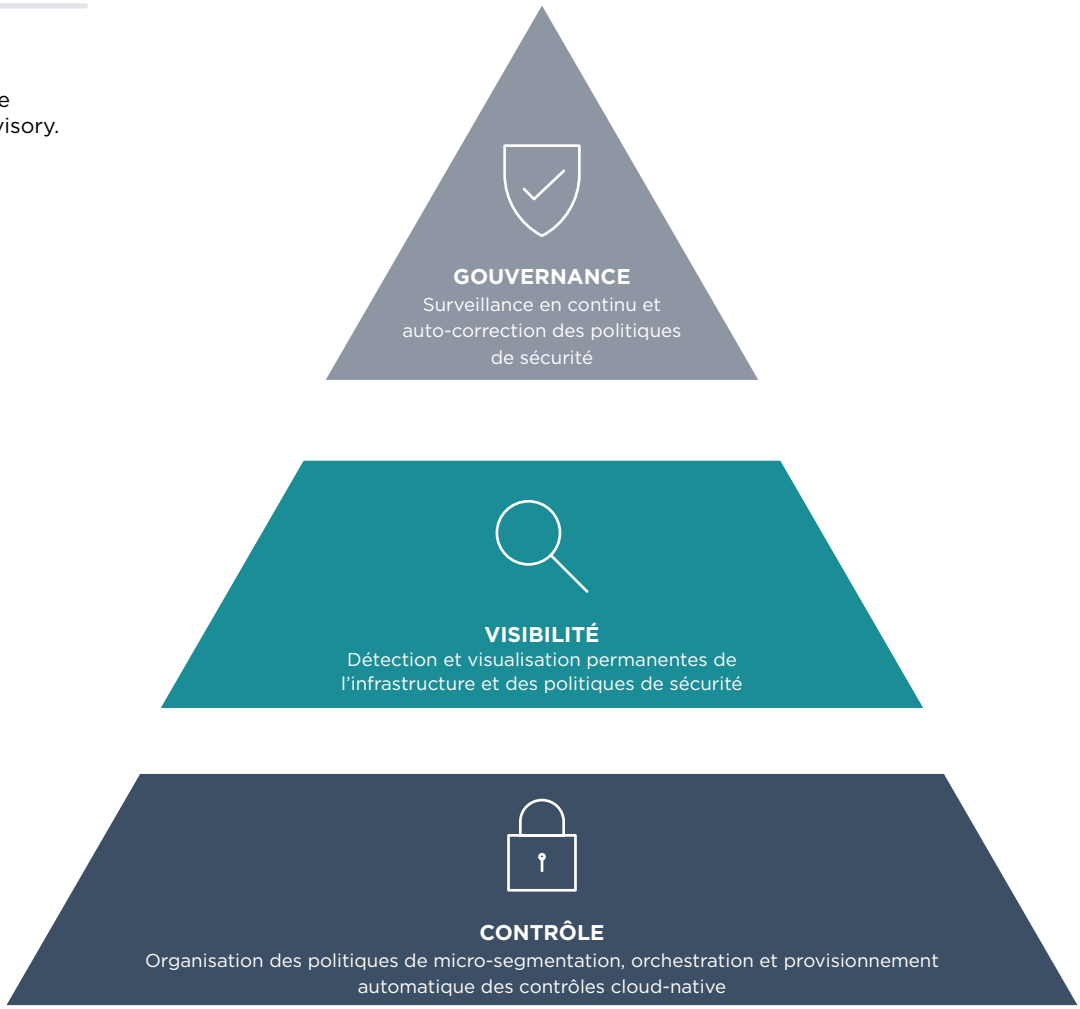
En appliquant les contrôles cloud-native et la micro-segmentation dans les règles de l'art, les workloads sont mieux protégés dans le cloud que dans les data centers traditionnels !

Cloudvisory : la solution tout-en-un

FireEye Cloudvisory permet une gestion et une orchestration puissantes et centralisées de la sécurité du cloud, capables d'exploiter les contrôles natifs des fournisseurs cloud.

Figure 1.

Composants de FireEye Cloudvisory.



Compatible avec les environnements AWS, Azure, GCP, Kubernetes, OpenStack et bare metal, Cloudvisory permet à votre entreprise d'accélérer ses opérations, de s'adapter aux changements dynamiques et de réduire les risques de compromission de sécurité.

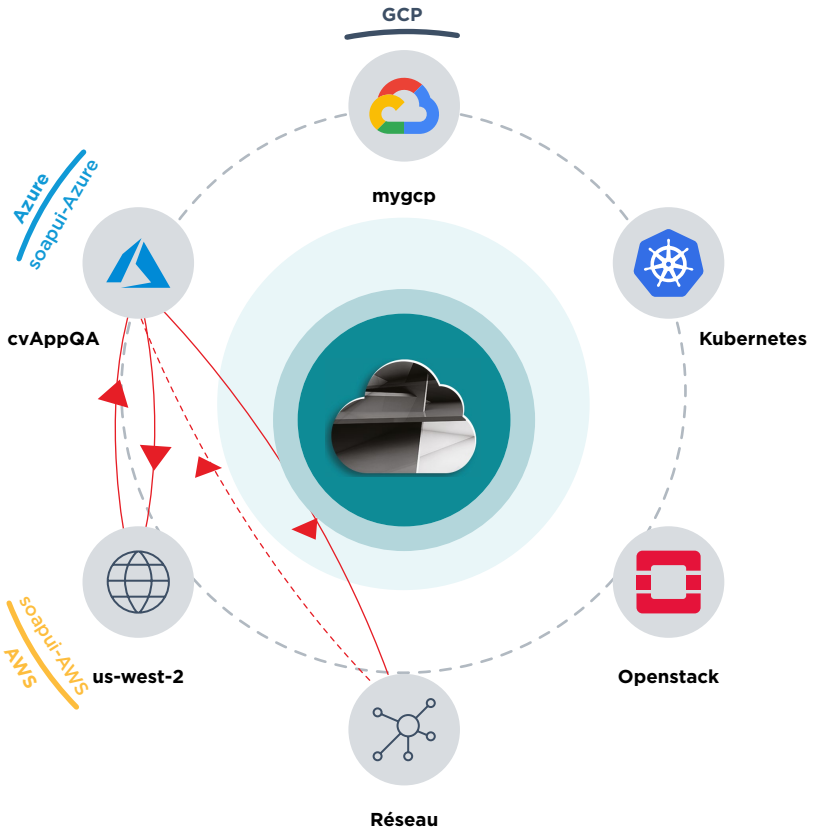
Visibilité cloud-native

Pour gérer, provisionner et corriger la sécurité des workloads, Cloudvisory identifie et topographie visuellement et continuellement l'infrastructure cloud-native et les objets de sécurité de chaque fournisseur cloud. Dans AWS par exemple, cela comprend les comptes, les régions, les VPC, les workloads, les groupes de sécurité et les flux de données réseau intra-workload. Dans OpenStack, on retrouve les comptes, les régions, les projets, les workloads, les groupes de sécurité et les flux de données.

Les flux de données sont mappés en temps réel, soumis aux contrôles de sécurité déployés, puis clairement définis comme conformes ou non conformes pour déterminer l'intégrité de l'état de l'environnement applicatif sous-jacent.

Figure 2.

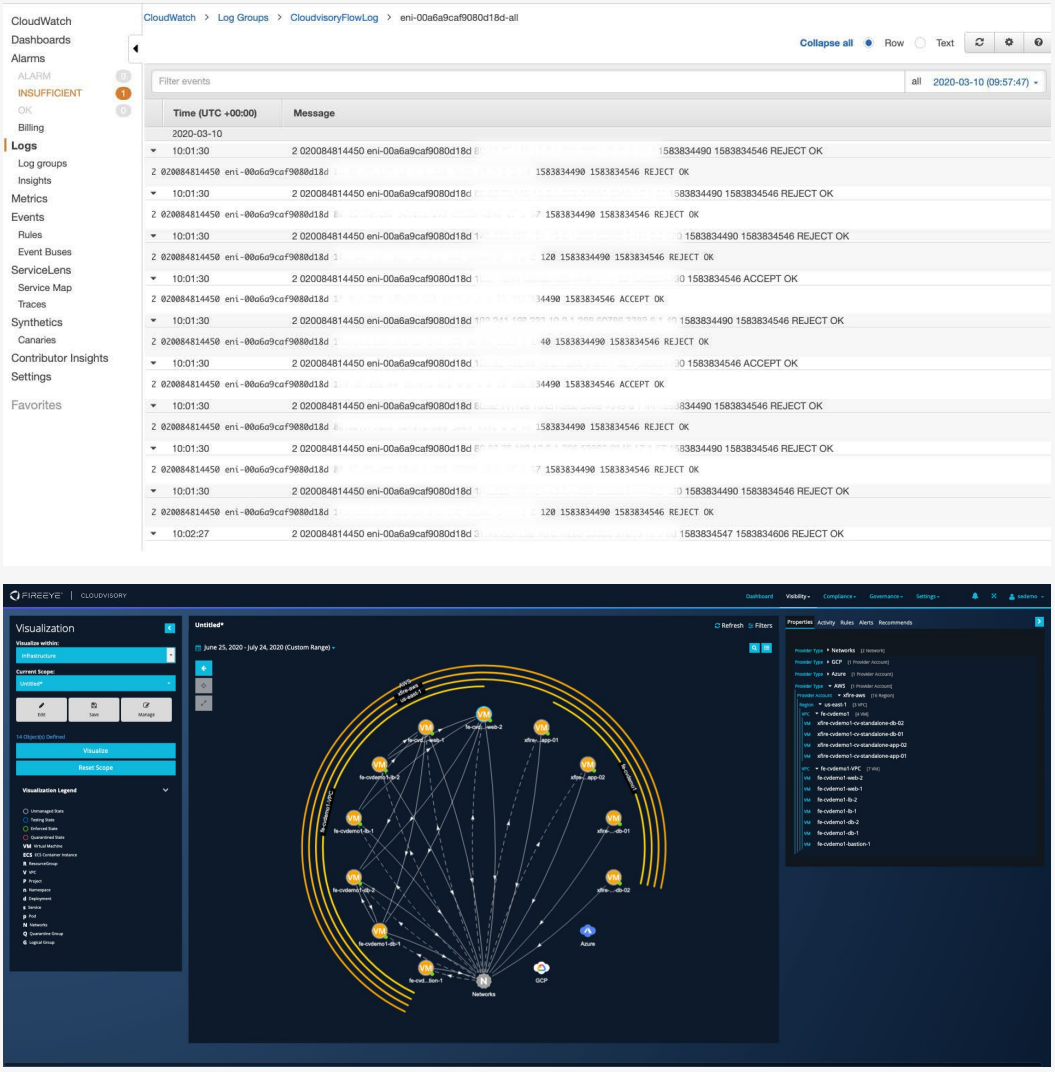
Visualisation Cloudvisory d'un environnement hybride comprenant AWS, Azure, GCP, OpenStack, Kubernetes et un data center classique.



Cloudvisory est capable d'actualiser les cartes visuelles à mesure que les ressources passent d'un environnement à un autre (du développement à la production) ou de l'on-prem au cloud (du data center à AWS), ou encore si l'environnement lui-même est modifié. Les équipes DevOps peuvent valider la politique en mode test, ce qui ne bloque pas les flux de données.

Figure 3.

Liste-type des flux VPC dans AWS (ci-dessus) pouvant être visualisés beaucoup plus clairement dans Cloudvisory (ci-dessous). Les comportements non conformes, tels que les attaques, peuvent être facilement détectés, signalés et mis en quarantaine.



Contrôle Cloud-Native

Pour créer, organiser et gérer des politiques de sécurité pour des environnements mono- ou multi-clouds, la solution idéale doit :

- Fournir une micro-segmentation granulaire et intelligente
- Simplifier la création de politiques à l'aide des contrôles de sécurité cloud-native
- Repérer les politiques mal configurées et aider à les corriger
- Organiser les contrôles de politiques pour une sécurité cohérente, répétable et inaltérable dans des environnements dynamiques
- Automatiser le provisionnement et le déprovisionnement précis des politiques sur l'ensemble des fournisseurs

Limites des anciennes méthodes de micro-segmentation

Les solutions de micro-segmentation classiques ont tendance à être très invasives et rigides, et ne prennent pas en charge les contrôles de sécurité cloud-native. De plus, leur dépendance au système d'exploitation (OS) ou aux pare-feu inline place le point de gouvernance de la sécurité à l'intérieur de la zone d'attaque, là où les malwares peuvent compromettre à la fois les workloads et les contrôles de sécurité. Enfin, les pare-feu inline augmentent la complexité de la configuration du cloud et posent des problèmes d'évolutivité.

Le manque de contrôles cloud-native oblige les clients à configurer manuellement tous les contrôles de sécurité des fournisseurs cloud. Ces derniers ne surveillent pas les points de gouvernance cloud-native, ce qui accroît les risques pour les entreprises. Quant aux changements accidentels ou non approuvés, ils peuvent exposer l'environnement au piratage et interrompre les applications actives.

Micro-segmentation intelligente

Il est tout à fait possible de passer à une micro-segmentation des workloads, des micro-services et des containers. L'implémentation d'un tel « réseau de workloads sécurisés », comme nous l'évoquions plus haut, est souhaitable à plusieurs égards :

- Les processus DevOps actuels appliquent souvent aux workloads des politiques de sécurité inadaptées ou trop permissives.
- Or, des droits d'accès excessifs accroissent considérablement les risques de malware et d'attaques par des groupes étatiques.
- Un malware qui peut facilement se déplacer latéralement dans l'environnement finira tôt ou tard par atteindre des données critiques.
- Les acteurs non autorisés peuvent être bloqués par les politiques de micro-segmentation.

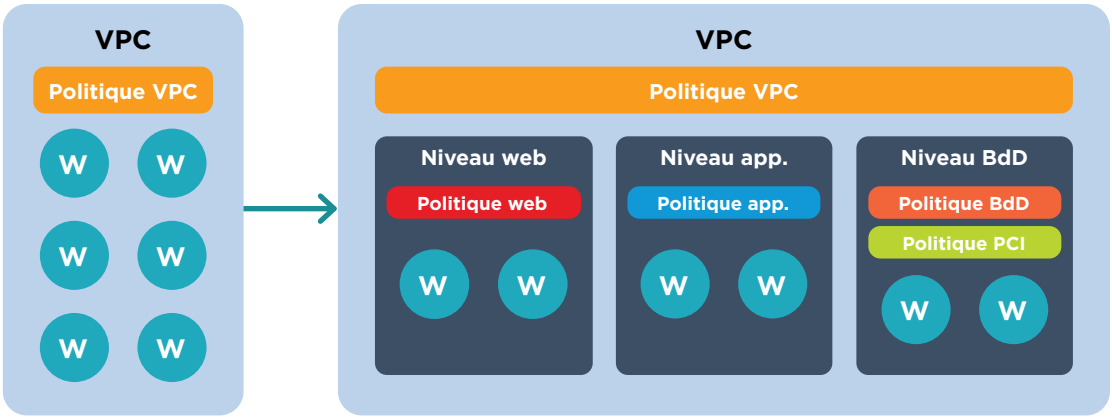
On voit donc que, lorsqu'elle est appliquée dans les règles de l'art, la micro-segmentation peut renforcer la sécurité et bloquer les mouvements latéraux en fractionnant les workloads en petits groupes isolés.

Liste blanche

Dans le cloud, les workloads ne peuvent pas recevoir de communications tant que les contrôles cloud-native ne sont pas configurés. Les politiques reposant sur les listes blanches permettent une entrée/sortie granulaire, ainsi que l'application de règles sur les ports et protocoles, ce qui dans les faits se traduit par un pare-feu au niveau des workloads (fig. 4). Ce type de protection des workloads met en échec les pirates et leurs tentatives de déplacement des malwares au sein de l'environnement. C'est pour cela que Cloudvisory permet d'activer des politiques de listes blanches en automatisant une micro-segmentation intelligente basée sur la gestion des politiques et l'infrastructure organisationnelle.

Figure 4.

Avant et après liste blanche.



Organiser et orchestrer les politiques de sécurité

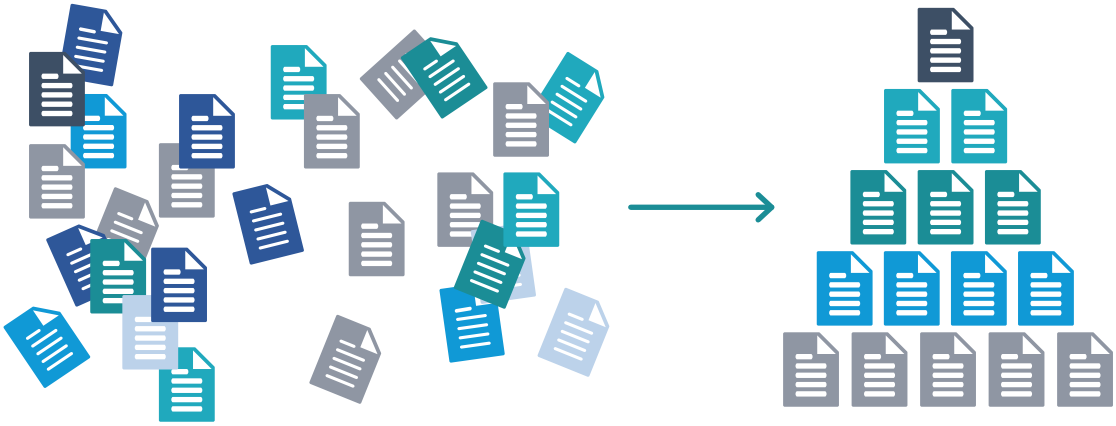
La puissance et l'évolutivité nécessaires à une bonne sécurisation des opérations cloud reposent largement sur l'organisation et l'orchestration de politiques de micro-segmentation.

Cloudvisory permet de répondre automatiquement aux changements dynamiques dans l'environnement, en ajustant les politiques de sécurité cloud-native en conséquence pour assurer la protection permanente des workloads. Pour organiser et gérer les politiques de façon flexible et agile, Cloudvisory s'appuie sur deux fonctionnalités :

- Détection automatique et groupement des workloads en fonction du contexte
- Création de politiques automatisée, faiblement couplées aux workloads via les groupes logiques

Figure 5.

Détection automatique et groupement des workloads en fonction de leur contexte.



Détection automatique du contexte des workloads

Les définitions de politiques sont associées aux workloads en fonction du contexte de ces derniers, ce contexte étant lui-même déterminé par les appartenances aux groupes logiques et englobant plusieurs variables :

- Fournisseur cloud
- Appartenance à une infrastructure
  - Compte
  - Région
  - Groupe de ressources, cloud privé virtuel, projet
- Application
  - Niveau applicatif
- Exigences de conformité telles que
  - CIS, GDPR, HIPAA, NIST, PCI, OpenStack Security Checklist, etc.
- Pratiquement tout groupement logique ou ad-hoc nécessaire à la gestion d'une politique

La fonction de détection continue permet à Cloudvisory d'identifier le contexte d'un workload et de grouper automatiquement les workloads dont les contextes se recoupent.

Création et gestion des politiques

Cloudvisory propose deux façons de créer des politiques. Ces méthodes sont toutes deux plus simples et plus précises que l'écriture de code au moyen d'outils d'orchestration disponibles sur le marché.

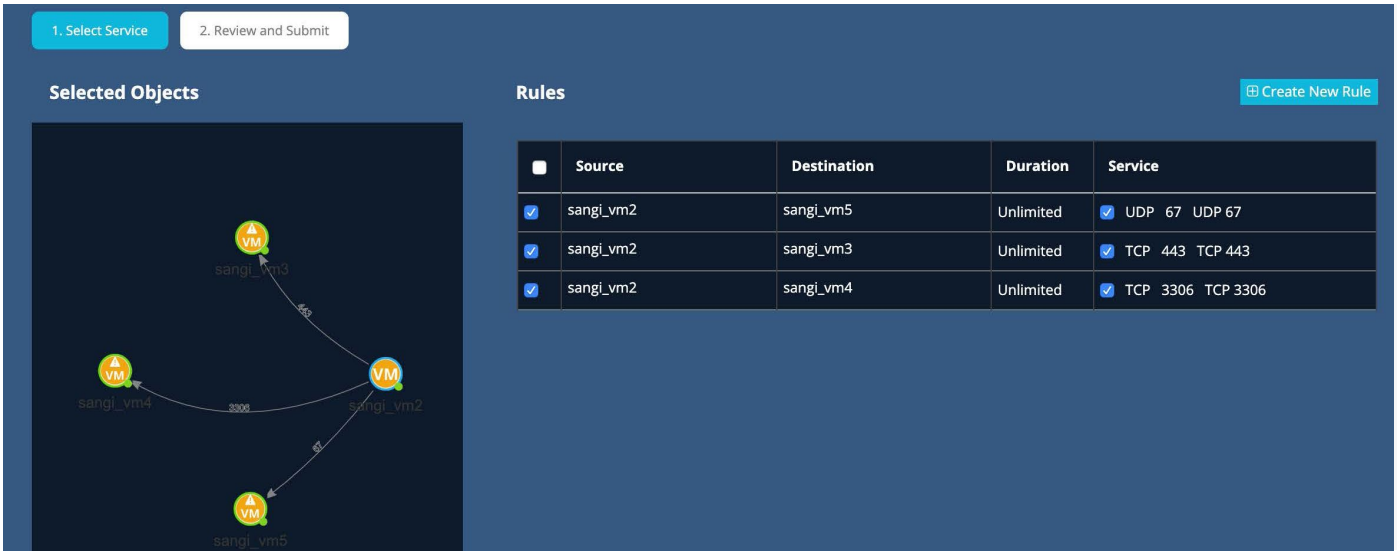
Création par pointer-cliquer

Avec Cloudvisory, nul besoin pour les utilisateurs d'être experts des contrôles natifs des fournisseurs cloud. Il suffit aux équipes DevOps de suivre une série d'écrans et d'effectuer quelques clics pour créer des politiques générales.

Identification des politiques

Souvent, les développeurs ne sont pas sûrs des règles exactes à implémenter pour contrôler une application spécifique. Cela peut se traduire par un accès trop permissif, et donc des risques accrus pour l'environnement. Cloudvisory est l'un des moyens les plus rapides de créer des politiques basées sur le principe du moindre privilège. Il peut définir les flux exacts requis pour exécuter une application et utiliser cette information pour créer des politiques exportables et réutilisables.

Figure 6. Écran de création des politiques de détection de Cloudvisory.



Quel que soit le mode de création des politiques, Cloudvisory traduit leurs définitions en contrôles cloud-native pour n'importe quel fournisseur de cloud. Imaginez une définition de politique PCI qui détermine quelles instances virtuelles peuvent communiquer avec l'infrastructure PCI dans le data center. Cloudvisory peut convertir cette définition en contrôles des différents fournisseurs, comme AWS Security Groups, Azure Network Security Groups et OpenStack Security Groups. Les paramètres réseau dynamiques tels que les adresses IP des serveurs ou les mouvements d'une application vers différents serveurs sont automatiquement gérés par Cloudvisory. Ces fonctionnalités évitent aux équipes DevOps de devoir se spécialiser dans les contrôles de chaque fournisseur, réduisant par là-même les besoins de codage associés.

Orchestration automatique

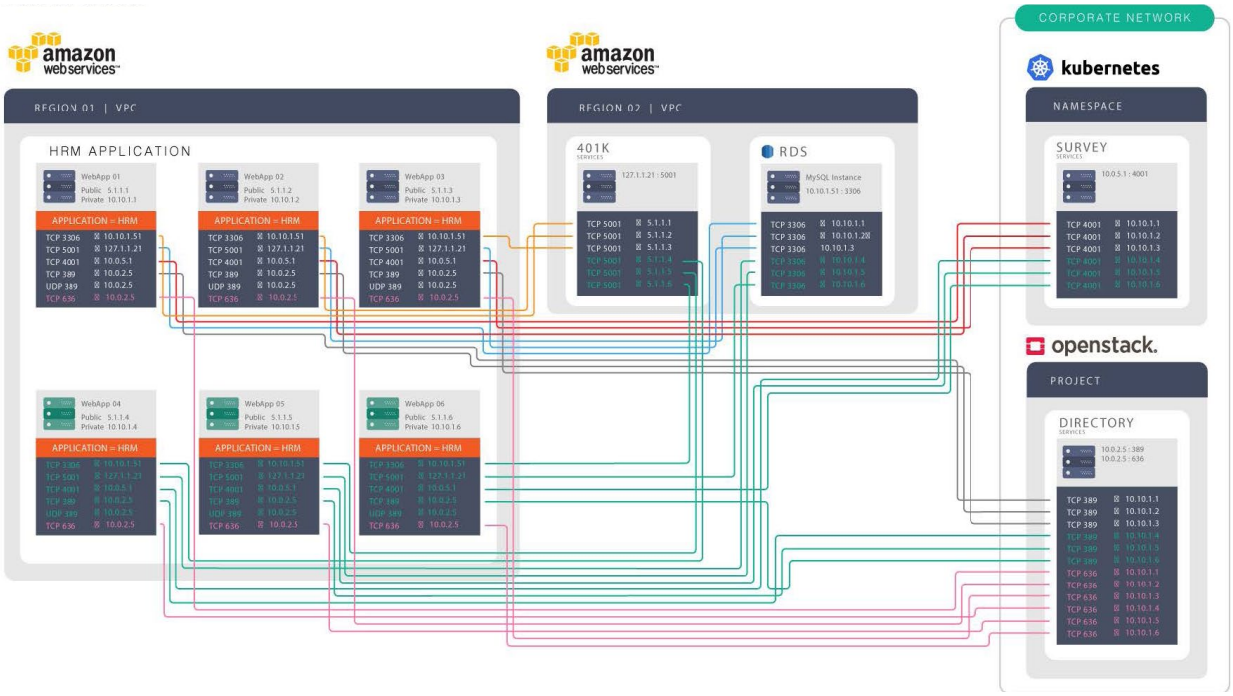
Une fois que Cloudvisory a établi les règles des politiques, elles sont faiblement couplées au contexte du workload à l'aide d'une API ou d'une interface de type pointer-cliquer. Il est alors possible de les provisionner de façon automatique et adaptée aux workloads, même lorsque de nouveaux workloads apparaissent, changent de rôle ou passent d'un environnement à un autre, d'un fournisseur à un autre ou d'un groupe logique à un autre. Dans chaque cas, Cloudvisory identifie automatiquement les changements de contexte et met à jour les politiques de sécurité en temps réel. Aucun codage ni script complexe n'est nécessaire, ce qui permet un meilleur contrôle de la sécurité et une gestion plus précise des politiques.

Gestion rapide des changements de politique

L'exemple ci-dessous, qui illustre un cloud hybride complexe comprenant des ressources AWS, Azure et OpenStack, permet de mettre en évidence la puissance de Cloudvisory.

Premièrement, la définition de la politique HRM créée par Cloudvisory pour l'application spécifie les règles de sécurité pour l'entrée et la sortie de tout workload contenant les métadonnées « app = HRM ». À mesure que de nouveaux workloads sont lancés avec ces métadonnées, Cloudvisory calcule et provisionne les contrôles cloud-native appropriés pour chaque service faisant partie de l'application HRM intégrée. Grâce au suivi de toutes les connexions requises, Cloudvisory met en place des politiques précises.

Figure 7. Cloud hybride complexe avec ressources réparties dans plusieurs environnements.



Les équipes DevOps chargées de coder ou de créer des scripts pour ces politiques doivent effectuer un suivi très complexe sur l'ensemble des environnements, adresses IP publiques et privées, ports et protocoles d'entrée et de sortie. Outre le fait qu'il est extrêmement chronophage, ce processus peut aboutir à des erreurs de configuration et des applications défaillantes. Cloudvisory automatise l'intégralité du processus et élimine toute la complexité liée à l'apprentissage, l'organisation, le provisionnement, le calcul, la mise à jour et la gestion des politiques de sécurité cloud-native. Résultat : gain de temps, allégement des coûts et sécurité plus cohérente et plus adaptée.

Surveillance et gouvernance

Une fois les politiques créées, organisées et provisionnées, il faut surveiller les environnements pour détecter d'éventuels compromis et éviter toute dérive des configurations de sécurité.

Grâce à l'interface Cloudvisory ou à ses API, les équipes business, opérationnelles ou sécurité peuvent visualiser le trafic des données sur les différents niveaux de la hiérarchie de l'infrastructure. Par exemple, l'utilisateur peut observer le trafic de données entre les machines virtuelles d'un même hyperviseur, entre différents fournisseurs cloud, entre le cloud et un data center traditionnel, ou dans un compte cloud unique. Contrairement aux collecteurs de flux classiques installés sur les commutateurs et les routeurs, les flux de données sont capturés, stockés et affichés avec des informations contextuelles (fournisseur, propriétés de l'infrastructure, application et attributs définis par l'utilisateur). Ce contexte transmet des informations qui permettent de mieux comprendre le comportement des applications, de corriger les politiques mal configurées, d'analyser et de trier rapidement les incidents de sécurité et de simplifier le traitement analytique des données.

Une fois l'infrastructure identifiée et les politiques définies, Cloudvisory assure une surveillance permanente dans deux domaines critiques :

- Les flux de données et le nombre d'octets de tous les workloads gérés
- Les points de gouvernance des politiques natives pour chaque workload

Violations des flux de données

Les flux de données sont analysés de façon à valider ou non leur conformité aux politiques déployées. Tout flux de données ne correspondant pas aux règles autorisées est immédiatement signalé comme non conforme, bloqué et clairement indiqué comme tel dans l'interface utilisateur.

Les alertes sont configurables et tout workload infecté peut être immédiatement mis en quarantaine pour neutraliser toute menace potentielle.

Par exemple, si un workload n'est pas autorisé à effectuer des transferts FTP et qu'il est infecté par un malware qui tente de d'extraire des données, Cloudvisory peut détecter la tentative de flux (avec l'augmentation du nombre moyen d'octets correspondant) et émettre une alerte sur cette activité. L'alerte est affichée sur le tableau de bord, envoyée sous forme de notification par email aux administrateurs et intégrée aux solutions SIEM. La tentative de communication se retrouve bloquée. Cloudvisory peut être configuré de façon à mettre immédiatement en quarantaine le workload infecté, à suspendre toutes les politiques de sécurité sortantes en cours et à bloquer l'ensemble du trafic réseau vers et depuis les workloads sélectionnés. Ces mesures empêchent le mouvement latéral des menaces vers d'autres applications et ressources, et toute autre infection du réseau jusqu'à ce que les équipes de sécurité puissent remédier à la situation.

Les alertes de trafic non conforme dues à des politiques mal configurées peuvent occasionner des dysfonctionnements dans les applications. Les administrateurs peuvent rapidement être informés de ces failles au niveau des politiques et les résoudre via l'interface pointer-cliquer.

Traitement automatique des violations

Cloudvisory vérifie en permanence la configuration des contrôles cloud-native pour s'assurer de leur conformité. Dès qu'une modification non autorisée dans les règles de sécurité est détectée, Cloudvisory génère une alerte. Les politiques de sécurité peuvent être configurées de manière à revenir automatiquement à l'état antérieur à la modification, ramenant ainsi les politiques à un état de conformité. Le cas échéant, il génère également une alerte et une entrée dans le journal d'audit pour consigner l'événement non conforme.

Prenons un exemple : un administrateur utilisant une console Azure supprime accidentellement les règles du groupe de sécurité pour l'accès au port 80. Chez de nombreux fournisseurs cloud, cet événement n'est pas signalé. Et pourtant il peut entraîner l'interruption d'une application due à l'impossibilité de contacter son interface web.

Cloudvisory est capable de détecter ces modifications de configuration accidentelles ou malveillantes, puis d'annuler immédiatement la modification pour ramener l'environnement à un état conforme et opérationnel. Cela réduit, voire élimine les interruptions de service, le tri automatisé et les risques.

Conclusion

Quels que soient leur taille et leur niveau de complexité, toutes les entreprises finissent par adopter des clouds privés et publics. Pour maintenir une sécurité en phase avec leurs opérations, elles doivent garder une excellente visibilité sur l'ensemble des surfaces d'attaque, adapter les configurations de sécurité à mesure que l'organisation évolue et bâtir une architecture de sécurité qui prenne en compte le caractère souple et dynamique du cloud.

Une telle stratégie implique d'agir sur plusieurs axes : l'orchestration et l'automatisation pour accélérer les opérations et minimiser les erreurs, la micro-segmentation pour implémenter des politiques centrées sur les workloads, la surveillance et la gouvernance pour identifier les risques et les menaces, et enfin la sélection de solutions tout-en-un capables de répondre à ces exigences.

Avec ses avantages hors pair – visibilité, gestion des politiques, puissance, simplicité d'utilisation – FireEye Cloudvisory propose une solution unique qui répond à tous ces impératifs de sécurité critiques pour les environnements cloud publics, privés et hybrides.

Pour en savoir plus, rendez-vous sur **www.fireeye.fr**

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™