PRÉSENTATION DE SOLUTION

Sécurité du cloud : renforcer la gouvernance des politiques

État des lieux
Automatiser la gouvernance des politiques n'est pas difficile en soi. Ce qui complique l'automatisation, ce sont les règles basées sur le principe du moindre privilège.

Passé un certain cap, la création de politiques respectant réellement ce principe peut s'avérer particulièrement complexe.

Il faut en effet une connaissance approfondie tant des contrôles de sécurité spécialisés que de l'environnement de déploiement, à savoir des comportements attendus et des relations entre différentes entités (systèmes, utilisateurs, services applicatifs, etc.) régies par un ensemble de contrôles donnés.

Or, les politiques réseau sont rarement créées par les personnes qui maîtrisent ces connaissances.

C'est là que l'intelligence artificielle entre en jeu. En alimentant l'IA avec les données d'API de fournisseurs cloud, il est possible de fournir aux machines le contexte nécessaire pour générer de meilleures politiques de sécurité basées sur le principe du moindre privilège, même à grande échelle.

L'intelligence artificielle au service d'une gouvernance renforcée des politiques
Chaque fournisseur cloud propose ses propres contrôles granulaires à base d'API pour la gouvernance des politiques basées sur le principe du moindre privilège. Même si ces contrôles de sécurité sont granulaires par essence, leur configuration laisse souvent à désirer. Plusieurs raisons à cela : commodité, inexpérience, voire malveillance, même lorsque leur provisionnement passe par des outils d'automatisation.

Les fournisseurs cloud offrent également différents services et fonctionnalités pour les déploiements éphémères et hyperscale. Les technologies matures d'automatisation des déploiements servent souvent à automatiser le déploiement des contrôles de sécurité et des ressources sous leur surveillance. Seulement voilà, ces contrôles de sécurité sont généralement mal configurés et rarement (voire jamais) soumis à des audits. On ne sait donc jamais si les configurations granulaires et le principe du moindre privilège sont réellement appliqués.

Côté développement, les organisations cherchent à préserver l'efficacité de leurs workflows DevOps basés sur des déploiements d'infrastructure éphémères et « as code » (IaC) avec orchestration et contrôle de version. Mais en même temps, elles ont aussi besoin que leurs équipes SecOps agissent au-delà de la simple amélioration de la visibilité. En clair, il est urgent de renforcer la supervision et la gouvernance à l'échelle de l'entreprise.

Une automatisation intelligente permettrait d'améliorer les workflows existants d'automatisation des déploiements à l'aide de politiques mieux définies et plus granulaires. Outre la neutralisation des menaces internes et externes, il en résulterait également une réduction des coûts.

Problèmes fondamentaux
Ces dix dernières années, les technologies d'automatisation des déploiements ont pris de vitesse les technologies d'automatisation de la sécurité sur tous les plans : adoption, fonctionnalités et maturité. C'est pourquoi, dans la plupart des ETI et grandes entreprises, les équipes DevOps (distribuées) gèrent leurs propres déploiements de façon autonome. Elles utilisent pour cela les solutions matures d'automatisation des déploiements de leur choix comme Ansible, Chef, CloudFormation, Puppet, Salt et Terraform, ou encore l'un des nombreux autres outils d'orchestration des déploiements de VM, containers et workloads via les API de leur fournisseur. Pour les équipes de sécurité, cela se

traduit par une perte de visibilité et de contrôle sur le comportement des ressources DevOps distribuées. À court terme, il est peu probable qu'elles utilisent leurs propres outils, si nouveaux soient-ils, pour reprendre le contrôle de la gouvernance DevOps.

La vérité, c'est que les équipes SecOps peinent à intégrer les outils d'automatisation DevOps. Certes, les technologies d'automatisation des déploiements permettent de créer et de reproduire un déploiement donné. Mais elles n'offrent aucune visibilité tangible sur le comportement des ressources sous gouvernance. Or, la gouvernance sans visibilité revient à faire confiance sans vérifier.

Les équipes SecOps doivent donc trouver le moyen d'éclairer ces zones d'ombre car, dans de nombreuses entreprises, les développeurs contrôlent la plupart des politiques de sécurité qui régissent les ressources cloud. Le modèle multi-locataire et self-service des technologies cloud a certes grandement amélioré l'efficacité et l'homogénéité des déploiements. Toutefois, les entreprises ont aussi appris à leurs dépens que les décisions de sécurité devraient être l'affaire de spécialistes. Nombre d'entre elles reconnaissent désormais qu'il leur faut de meilleurs garde-fous pour garantir la viabilité de ces modèles sur le long terme.

Même si les équipes SecOps parviennent à éliminer les angles morts et à obtenir le contexte nécessaire pour réellement appliquer le principe du moindre privilège, plusieurs problématiques subsisteront. Si la question du contexte mobilise trop de ressources en termes humains, il sera impossible de monter en capacité sur de grands environnements cloud. Il n'est pas non plus envisageable de confier le contrôle des ressources en production aux seules machines. Il faudra donc trouver le juste équilibre entre automatisation et humain.

Critères de la solution idéale

Les solutions de gouvernance doivent fournir une bonne visibilité sur la configuration et les comportements des ressources prises en charge. Il en va de votre capacité à analyser et améliorer en continu les performances de ces activités de gouvernance. La difficulté ne tient pas tant dans l'automatisation de la gouvernance des politiques que dans le choix des politiques de sécurité à automatiser (politiques basées sur le principe du moindre privilège, bien sûr).

Étant donné que de nombreuses entreprises utilisent déjà des technologies matures d'automatisation des déploiements, une solution de gouvernance doit surtout automatiser la création de meilleures politiques de gouvernance. Elle doit également pouvoir émettre des recommandations de politiques avisées sans rien modifier en dehors des pipelines standards d'automatisation des déploiements.

Une solution de gouvernance a pour principale vocation de renforcer (et non de remplacer) les contrôles existants grâce à de meilleures données sur les politiques. De fait, la création de meilleures politiques de gouvernance nécessite une visibilité étendue sur tout le contexte d'un ensemble de ressources données. Le machine learning s'appuie sur ces informations contextuelles pour modéliser les comportements des ressources au fil du temps. Plus le contexte est riche, plus le modèle sera complet. Et meilleures seront les politiques générées. Par conséquent, une bonne solution de gouvernance doit automatiser la collecte, le traitement et la corrélation des différentes couches de contexte utilisées pour modéliser et comprendre les comportements des ressources.

La solution idéale s'appuiera donc sur l'intelligence artificielle (IA) et son pendant, le machine learning, pour automatiser l'extraction de données contextuelles détaillées sur les ressources à partir des API des fournisseurs cloud. Elle utilisera l'intégralité de ce contexte pour déterminer le dosage idéal de principe du moindre privilège à appliquer à ces ressources. Ces politiques créées par IA serviront à leur tour à renforcer les outils et processus de gouvernance existants. Enfin, la solution devra permettre d'exporter les recommandations de politiques dans un format natif utilisable pour actualiser un référentiel d'infrastructure IaC avec contrôle de version, ou mettre à jour les politiques de sécurité d'un déploiement donné à l'aide d'un outil existant d'automatisation des déploiements.

La solution Cloudvisory

Le volet gouvernance de Cloudvisory communique directement avec les API des fournisseurs cloud pour vous offrir une gouvernance cloud-native des politiques. Sans recourir à des agents basés sur les workloads, cette solution automatise entièrement la collecte, le traitement et l'analyse de base des événements de sécurité des workloads et services, et ce à travers de multiples comptes et fournisseurs cloud. Elle détecte également en temps réel les modifications apportées à l'inventaire des ressources et aux configurations de sécurité. Ainsi, les utilisateurs peuvent personnaliser leur réponse (alerte, rollback, remédiation, etc.) aux infractions de politiques détectées.

Cloudvisory vous donne les moyens d'entamer votre transition vers une gouvernance basée sur le principe du moindre privilège en vous aidant à éliminer les angles morts et à maintenir votre conformité dans une démarche d'amélioration de vos pratiques de gouvernance. Elle s'appuie également sur le contexte système, cloud, historique et de sécurité d'une ressource donnée pour modéliser automatiquement ses comportements attendus.

Cloudvisory repose sur le machine learning pour automatiser les tâches difficiles et coûteuses de création de politiques basées à la fois sur le principe du moindre privilège et sur les contraintes des ressources en question. Si cette solution fournit un moteur

complet d'orchestration des politiques pour appliquer la microsegmentation réseau et d'autres règles de sécurité basées sur le fameux principe, elle permet également aux utilisateurs de sélectionner les outils de gouvernance et d'orchestration de leur choix. Enfin, Cloudvisory est suffisamment puissante pour couvrir de grands déploiements multicloud basés exclusivement sur le principe du moindre privilège. Elle est aussi suffisamment flexible pour permettre aux utilisateurs de renforcer leurs processus de gouvernance existants à l'aide de politiques mieux adaptées.

Pourquoi Cloudvisory
Cloudvisory résout efficacement les problèmes cloud complexes des entreprises.

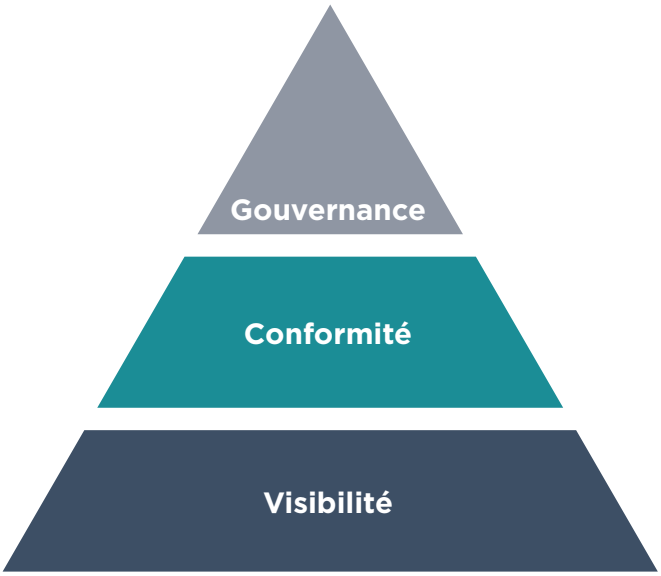
Les produits concurrents promettent beaucoup, mais les résultats sont souvent décousus et limités dans leur portée. De nombreuses alternatives ne prennent en charge que des fournisseurs de cloud public comme Kubernetes et OpenStack. Les soi-disant « solutions multicloud » sont souvent basées sur des agents et dépendantes des terminaux (systèmes d'exploitation), ce qui n'a rien de cloud-native et ne fournit généralement aucun contexte cloud.

Systémiques par nature, les problèmes les plus complexes nécessitent des solutions exhaustives. À cet égard, Cloudvisory est la seule à offrir une gouvernance cloud-native et multicloud complète. Seule Cloudvisory assure une gouvernance sans agent transverse aux environnements de cloud public et privé comme AWS, Azure, Google Cloud, Kubernetes et OpenStack.

Toutefois, même une solution techniquement complète pourra ne pas suffire. En effet, elle doit aussi opérer en synergie avec les processus et les professionnels qui l'implémentent. C'est pourquoi Cloudvisory permet aux entreprises et unités opérationnelles d'implémenter des politiques de gouvernance en phase avec leurs propres pratiques et exigences.

Avec Cloudvisory, vous pouvez à la fois conserver vos outils d'automatisation existants et capitaliser sur le machine learning pour renforcer la gouvernance de vos politiques de sécurité.

L'union fait la force
La gouvernance Cloudvisory s'appuie sur les fonctionnalités de visibilité et de conformité de la même solution pour assurer une gouvernance cloud-native et intelligente d'environnements multicloud dynamiques et complexes. Les algorithmes ML de Cloudvisory se nourrissent des données contextuelles détaillées de ces fonctionnalités afin d'assimiler un maximum d'informations système, cloud, historiques et de sécurité sur la ressource concernée. Ce contexte enrichi se traduit par des politiques de gouvernance plus précises. L'intelligence artificielle intégrée à Cloudvisory facilite et accélère la création de telles politiques.



Sécurité du cloud : garantir le maintien de la conformité

Sécurité du cloud : la fin des angles morts

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 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™