Guide de sécurisation des plateformes cloud

Table des matières

Enseignements-clés

1. Idéalement, un fournisseur de cloud doit pouvoir intégrer dans sa plateforme le système de gestion des identités de votre entreprise – et en tout cas mettre à votre disposition une solution de gestion des identités fiable.

2. Dans le cadre de l'établissement de la confiance, vérifiez qu'une plateforme cloud offre des pare-feux bien intégrés, des groupes de sécurité ainsi que des options de microsegmentation basées sur les charges de travail et des hôtes de calcul dignes de confiance.

3. Exigez d'un fournisseur de cloud qu'il propose des solutions BYOK (bring your own key), qui laissent à votre entreprise la gestion exclusive des clés pour tous les services et systèmes de stockage de données.

4. Pour ce qui est des conteneurs, la meilleure pratique de sécurité consiste à les analyser avant leur déploiement et pendant leur fonctionnement pour détecter leurs éventuelles vulnérabilités.

5. Le système de sécurité d'une plateforme cloud doit efficacement contrôler les accès, opérer au niveau des charges de travail, suivre l'activité de façon détaillée et s'intégrer avec les systèmes sur site.

Repenser la sécurité des applications cloud

Alors que de plus en plus d'entreprises adoptent un modèle « cloud natif » pour développer leurs applications et gérer leurs charges de travail, les plateformes cloud atteignent rapidement les limites de l'efficacité du traditionnel modèle de sécurité basé sur le périmètre. Bien qu'elle demeure nécessaire, la sécurité périmétrique seule est insuffisante. Comme les données et applications résidant dans le cloud sont situées en dehors des anciennes limites de l'entreprise, il faut trouver de nouvelles façons de les protéger.

Les entreprises qui adoptent un modèle « cloud natif » ou qui projettent de déployer des applications dans un cloud hybride doivent compléter leur sécurité réseau périmétrique par des technologies qui protègent les charges de travail hébergées dans le cloud. Les entreprises doivent faire confiance à la manière dont leur fournisseur de services cloud sécurise leur pile applicative en partant du niveau de l'infrastructure. La confiance dans la sécurité de la plateforme est devenue un critère essentiel pour le choix d'un fournisseur.

Facteurs de sécurisation du cloud

La protection des données et le respect de la réglementation font partie des principaux facteurs de sécurisation du cloud – mais elles sont aussi des obstacles à l'adoption de ce dernier. Dissiper ces préoccupations doit être une priorité dans tous les aspects du développement et des opérations. Avec les applications cloud natives, les données peuvent être réparties entre plusieurs magasins d'objets, services de données et clouds, qui sont autant de nouveaux fronts ouverts aux attaques potentielles. Et les attaques ne sont pas seulement le fait de sources externes et de cybergangs sophistiqués : lors d'une étude récente, 53 % des répondants ont déclaré avoir subi des attaques internes au cours des 12 derniers mois[1].

Cinq mesures essentielles de sécurisation du cloud

Lorsque les entreprises mettent en place les mesures de sécurité spécifiques qu'impose l'utilisation d'une plateforme cloud, elles ont besoin que leurs fournisseurs deviennent des partenaires technologiques de confiance. En fait, elles doivent évaluer les fournisseurs de cloud sous les cinq angles de sécurité suivants, à la lumière de leurs besoins spécifiques :

1. **Gestion des accès et des identités :** Authentification, contrôles des identités et des accès
2. **Sécurité du réseau :** Protection, isolation et segmentation
3. **Protection des données :** Chiffrement des données et gestion des clés
4. **Sécurisation des applications et DevSecOps :** Inclut les tests de sécurité et la sécurisation des conteneurs
5. **Visibilité et intelligence :** Surveillance et analyse des journaux, flux et événements afin d'y détecter des schémas

Vérifier les identités et gérer l'accès sur une plateforme cloud

Toute interaction avec une plateforme cloud commence par une vérification d'identité afin d'établir qui, ou ce qui, est à l'origine de l'interaction : un administrateur, un utilisateur, voire un service. Dans l'économie des API, les services ont leur propre identité ; pouvoir effectuer de façon précise et sûre un appel d'API à un service en utilisant cette identité est donc essentiel pour une bonne exécution des applications cloud natives.

Recherchez des fournisseurs qui proposent un moyen cohérent d'authentifier une identité en vue d'accéder à des API et d'effectuer des appels de service. Il vous faut également un moyen d'identifier et authentifier les utilisateurs finaux qui accèdent à vos applications hébergées dans le cloud. Par exemple, IBM Cloud utilise App ID pour permettre aux développeurs d'intégrer l'authentification dans leurs applications mobiles et web.

L'authentification forte empêche les utilisateurs non autorisés d'accéder aux systèmes cloud. Puisque la gestion des accès et des identités (IAM) est si cruciale sur les plateformes, les entreprises qui disposent déjà d'un système de gestion des identités doivent exiger de leurs fournisseurs qu'ils l'intègrent au leur. Cette intégration s'effectue souvent à l'aide d'une technologie de fédération d'identité, qui lie l'ID et les attributs d'un individu sur plusieurs systèmes.

Pourquoi authentifier les appels de service ?

Dans les architectures à base de microservices, les API permettent aux applications de communiquer et de partager des données. Quand une application s'exécute, elle utilise des API pour appeler les services dont elle a besoin pour effectuer différentes opérations. Par exemple, votre application peut appeler un service de magasin d'objets afin d'obtenir des données. Pour répondre à sa demande, ce service peut à son tour appeler un service de gestion de clés afin d'obtenir les clés de chiffrement requises pour déchiffrer les données. Et pour offrir son expérience utilisateur, une application peut utiliser des API pour accéder aux informations d'identité des utilisateurs, publier du contenu sur d'autres applications (par exemple, sur Twitter) et pour déterminer l'emplacement d'un utilisateur afin de lui fournir des informations locales. **Tous ces points d'intégration posent des problèmes de sécurité.**

Les fournisseurs de cloud doivent disposer d'un moyen cohérent d'authentifier l'identité d'un utilisateur ou d'un service qui a besoin d'accéder à une API ou à un service. Bien sûr, dans le cadre de l'authentification, toutes les sessions et transactions de demande d'accès doivent être consignées aux fins d'audit. **Vos API et services renferment très probablement une propriété intellectuelle précieuse ; ne laissez pas n'importe qui les utiliser.**

Demandez aux fournisseurs de cloud que vous étudiez de vous prouver que leurs systèmes et leur architecture IAM répondent à toutes ces exigences de base. Dans IBM Cloud, par exemple, la gestion des accès et des identités repose sur plusieurs fonctionnalités-clés (Figure 1) :

Identité

- Chaque utilisateur possède un identificateur unique.
- Les services et les applications sont identifiés par leur ID de service.
- Les ressources sont identifiées et appelées par leur nom de ressource de cloud (CRN).
- Les utilisateurs et les services sont authentifiés et reçoivent des jetons comportant leur identité.

Gestion des accès

- Lorsque les utilisateurs et les services tentent d'accéder à des ressources, un système IAM détermine si les accès et actions doivent être autorisés ou refusés.
- Des services définissent les actions, les ressources et les rôles.
- Les administrateurs définissent les règles qui affectent aux utilisateurs des rôles et des droits sur les ressources.
- La protection s'étend aux API, aux fonctionnalités cloud et aux ressources de back end hébergées dans le cloud.

Lorsque vous évaluez l'offre de sécurité d'un fournisseur de cloud, recherchez la présence des ACL (liste de contrôle d'accès) et des noms de ressources communs, qui vous permettent d'autoriser les utilisateurs à accéder à certaines ressources uniquement et à effectuer certaines opérations seulement sur ces ressources. Ces fonctionnalités contribuent à garantir que vos données sont protégées contre les accès non autorisés externes ou internes.

Étendre votre propre fournisseur d'identité d'entreprise au cloud est particulièrement utile quand vous construisez une application cloud native au-dessus d'une application d'entreprise existante qui utilise ce fournisseur d'identité. Vos utilisateurs peuvent alors se connecter sans difficulté à ces deux applications sans devoir utiliser plusieurs systèmes ou ID. Il est toujours utile de réduire la complexité.

Enseignement-clé

Idéalement, un fournisseur de cloud doit pouvoir intégrer dans sa plateforme le système de gestion des identités de votre entreprise – et en tout cas mettre à votre disposition une solution de gestion des identités fiable.

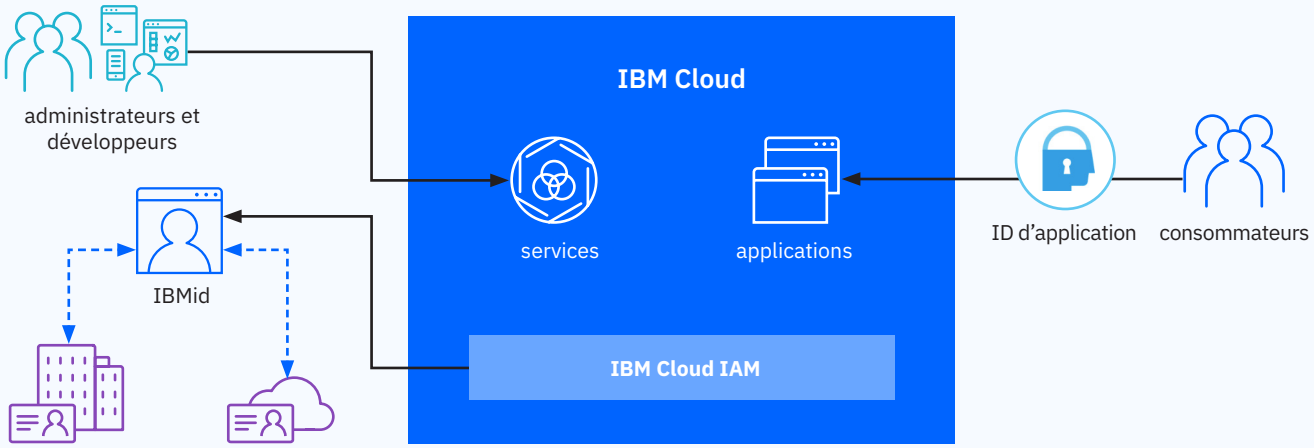


Figure 1. Séparation entre les éléments de cluster gérés par le fournisseur et ceux gérés par le client.

Redéfinir l'isolation et la protection du réseau

De nombreux fournisseurs de cloud utilisent la technique de la segmentation du réseau pour limiter l'accès aux équipements et serveurs d'un même réseau. En outre, ils créent des réseaux isolés virtuels sur l'infrastructure physique et restreignent automatiquement les utilisateurs ou les services à un réseau isolé spécifique. Ces méthodes, ainsi que d'autres techniques de base de sécurisation des réseaux, sont leur outil de base pour instaurer la confiance sur une plateforme cloud.

Les fournisseurs de cloud proposent des technologies de protection – qui vont des pare-feux d'application web aux réseaux privés virtuels et à l'atténuation du refus de service – sous forme de services pour offrir une sécurité des réseaux définie par logiciels, et facturent à l'utilisation. À l'ère du « cloud computing », les technologies ci-après doivent être considérées comme indispensables pour la sécurité des réseaux.

Groupes de sécurité et pare-feux

Les utilisateurs de cloud insèrent souvent des pare-feux réseau pour assurer la protection périmétrique (cloud privé virtuel/accès réseau au niveau d'un sous-réseau) et créent des groupes de sécurité réseau pour un accès au niveau instance. Les groupes de sécurité constituent une bonne première ligne de défense pour attribuer l'accès aux ressources cloud. Ils permettent de mettre facilement en place une sécurité réseau au niveau instance afin de gérer le trafic entrant et sortant dans les réseaux publics comme dans les réseaux privés.

De nombreux clients ont besoin d'un contrôle périmétrique pour sécuriser leurs réseaux périmétriques et leurs sous-réseaux, et les pare-feux virtuels sont un moyen aisément déployable de répondre à cette exigence. Les pare-feux sont conçus pour empêcher tout trafic indésirable d'atteindre les serveurs et réduire ainsi le périmètre de vulnérabilité. Recherchez des fournisseurs de cloud qui proposent des pare-feux virtuels et des pare-feux matériels vous permettant de configurer des règles basées sur les droits pour la totalité du réseau ou pour des sous-réseaux.

Bien entendu, les VPN (réseaux privés virtuels), offrent des connexions sécurisées entre le cloud et vos ressources locales. Vous devez en créer si vous utilisez un environnement de cloud hybride.

Microsegmentation

Développer des applications cloud natives sous forme d'ensembles de petits services offre l'avantage en termes de sécurité de pouvoir les isoler à l'aide de segments de réseau. Recherchez une plateforme cloud qui met en œuvre la microsegmentation via l'automatisation de la configuration et de la mise à disposition du réseau. **Les applications conteneurisées architecturées sur le modèle des microservices sont rapidement en passe de devenir la norme pour supporter une isolation évolutive des charges de travail.**

Enseignement-clé

Dans le cadre de l'établissement de la confiance, vérifiez qu'une plateforme cloud offre des pare-feux bien intégrés, des groupes de sécurité ainsi que des options de microsegmentation basées sur les charges de travail et des hôtes de calcul dignes de confiance.

Protéger les données grâce au chiffrement et à la gestion des clés

Protéger ses données de façon fiable est un impératif de sécurité pour toute entreprise numérique – surtout celles qui opèrent dans des secteurs fortement réglementés, tels que ceux des services financiers et de la santé.

Les données des applications cloud natives peuvent être réparties entre plusieurs magasins d'objets, services de données et clouds. Les applications traditionnelles peuvent avoir leur propre base de données, leur propre machine virtuelle ainsi que des données sensibles stockées dans des fichiers. Il est alors crucial de chiffrer ces données sensibles, qu'elles soient au repos ou en transit.

Les entreprises ont raison de s'inquiéter du risque que les opérateurs de cloud et autres utilisateurs non autorisés accèdent à leurs données à leur insu, et d'exiger une visibilité complète sur les accès à leurs données. **Contrôler l'accès aux données grâce au chiffrement et contrôler l'accès aux clés de chiffrement deviennent des mesures de protection qui doivent être proposées.** Par conséquent, le modèle BYOK (bring your own key) est désormais indispensable pour la sécurisation des clouds. Il vous permet de gérer vos clés de chiffrement de façon centralisée, garantit que les clés racines ne quittent jamais le système de gestion des clés et vous permet d'auditer toutes les activités de gestion des clés (Figure 2).

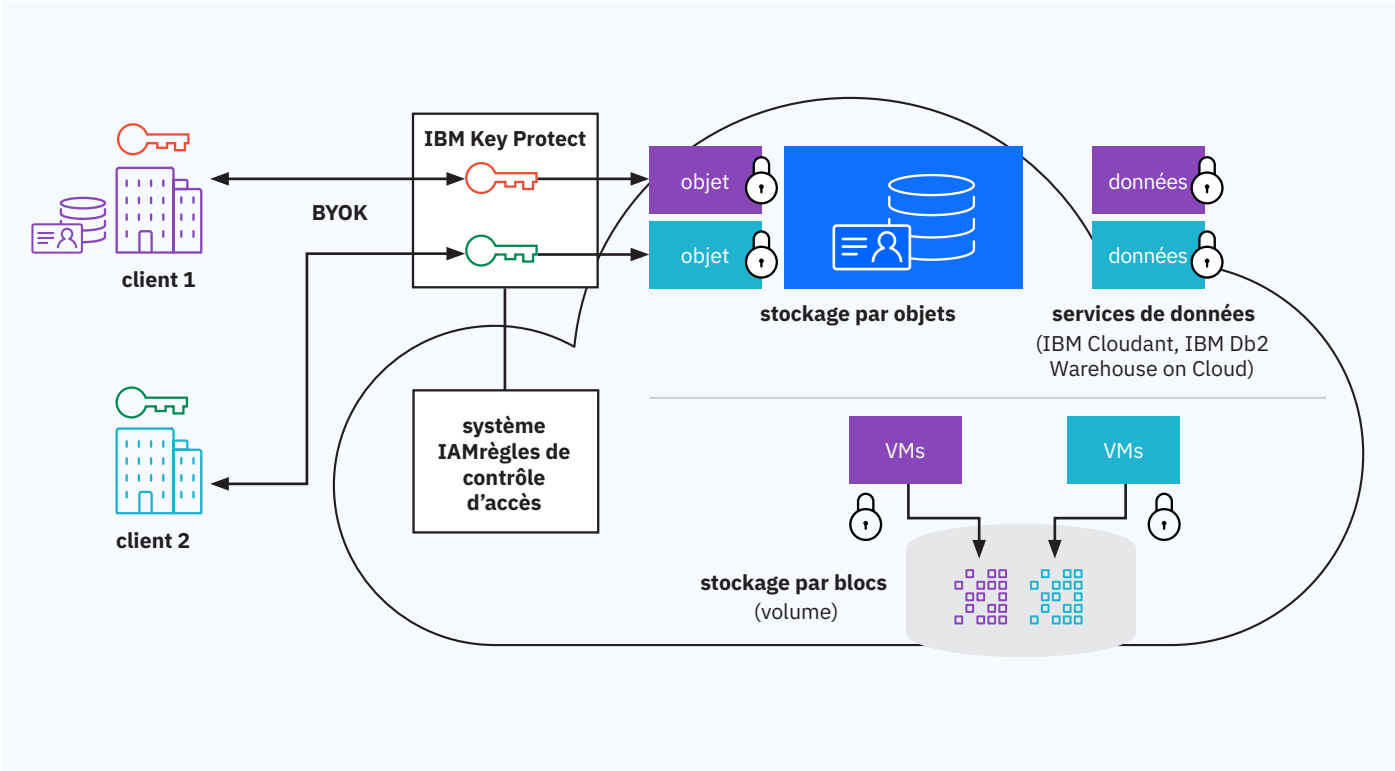
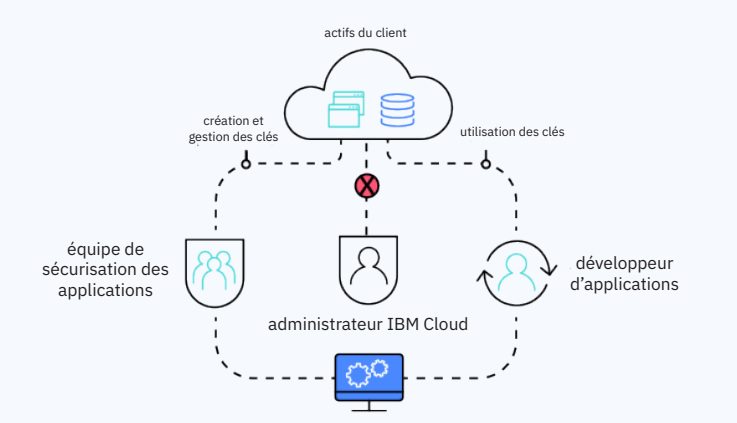


Figure 2. Architecture d'une solution BYOK.

KYOK (keep your own key)

Pour mettre en œuvre une sécurité des données qui reste 100 % privée dans le cloud public, IBM propose en exclusivité une solution qui vous permet d'être l'unique détenteur de votre clé de chiffrement. Seul service du marché reposant sur du matériel certifié FIPS 140-2 Level 4, IBM Cloud Hyper Protect Crypto Services est un service de gestion des clés et un module de sécurité matérielle (HSM) cloud.



Hôtes de calcul dignes de confiance

Tout est une question de matériel : personne ne veut déployer des applications et des données précieuses sur un hôte non sécurisé. Les fournisseurs de plateformes cloud qui proposent du matériel avec des protocoles mesurer-vérifier-démarrer offrent des hôtes très sécurisés pour les applications déployées dans le système d'orchestration de conteneurs.

Intel Trusted Execution Technology (Intel TXT) et Trusted Platform Module (TPM) sont deux exemples de technologies de niveau hôte qui sécurisent les plateformes cloud. Intel TXT protège contre les attaques logicielles qui cherchent à dérober des informations sensibles en endommageant le code du système ou du BIOS ou en modifiant la configuration de la plateforme. Intel TPM est un dispositif de sécurité matériel qui aide à protéger le processus de démarrage du système, en s'assurant qu'il n'a pas été altéré avant de transmettre le contrôle du système au système d'exploitation.

Protection des données au repos et en transit

Le chiffrement intégré avec BYOK vous permet de conserver le contrôle de vos données sur site ou dans le cloud. C'est un excellent moyen de contrôler l'accès aux données dans les déploiements d'applications cloud natives. Avec cette approche, le système de gestion des clés du client génère une clé sur site et la transmet au service de gestion des clés du fournisseur. Cette approche englobe le chiffrement des données au repos pour tous les types de stockage (par blocs, par objets et par services de données).

Pour les données en transit, la communication et le transfert s'effectuent sur une liaison Transport Layer Security/Secure Sockets Layer (TLS/SSL). Le chiffrement TLS/SSL vous permet également d'apporter la preuve de la conformité, de la sécurité et de la gouvernance sans être obligé de mettre en place un contrôle administratif du système cryptographique ou de l'infrastructure. La possibilité de gérer les certificats SSL constitue un impératif pour qu'une plateforme cloud soit digne de confiance.

Répondre aux besoins d'audit et de conformité

Fournir vos propres clés de chiffrement et les conserver dans le cloud – sans qu'aucun fournisseur de services n'y accède – vous offre la visibilité et le contrôle sur les informations exigés lors des audits de conformité des responsables de la sécurité des systèmes d'information (RSSI).

Enseignement-clé

Exigez d'un fournisseur de cloud qu'il propose des solutions BYOK, qui laissent à votre entreprise la gestion des clés pour tous les services et systèmes de stockage de données.

Automatiser la sécurité pour DevOps

Lorsque les équipes DevOps construisent des services cloud natifs et utilisent les technologies basées sur les conteneurs, elles doivent pouvoir intégrer les contrôles de sécurité dans un pipeline de plus en plus automatisé. Étant donné que des sites tels que Docker Hub favorisent les échanges ouverts, les développeurs peuvent facilement économiser du temps de préparation des images en téléchargeant simplement ce dont ils ont besoin. Mais cette flexibilité impose d'inspecter systématiquement toutes les images de conteneur placées dans un registre avant de les déployer.

Un système d'analyse automatisé aide à garantir que ces images sont dignes de confiance en recherchant leurs vulnérabilités potentielles avant toute utilisation. Demandez à vos fournisseurs de plateformes s'ils autorisent votre entreprise à créer des règles (telles que « ne pas déployer une image présentant des vulnérabilités » ou « m'avertir avant de déployer ces images en production ») dans le cadre de la sécurisation du pipeline DevOps.

IBM Cloud Container Service, par exemple, propose un outil de conseil concernant les vulnérabilités, baptisé Vulnerability Advisor (VA), qui est capable d'analyser les conteneurs de façon statique ou dynamique. VA inspecte chaque couche de chaque image dans le registre privé d'un client cloud afin de détecter les vulnérabilités ou les logiciels malveillants avant le déploiement des images. Comme une simple analyse des images du registre peut échouer à détecter des problèmes tels que des différences entre l'image statique et les conteneurs déployés, VA analyse aussi les conteneurs actifs pour y rechercher d'éventuelles anomalies. Il fournit également des recommandations sous forme d'alertes graduées.

Enseignement-clé

Pour ce qui est des conteneurs, la meilleure pratique de sécurité consiste à les analyser avant leur déploiement et pendant leur fonctionnement pour rechercher leurs éventuelles vulnérabilités.

Autres fonctionnalités de VA qui aident à automatiser la sécurisation du pipeline DevOps :

- **Paramètres de violation des règles :** Avec VA, les administrateurs peuvent définir des règles de déploiement d'image basées sur trois types de situations de défaillance d'une image : packages installés présentant des vulnérabilités connues, connexions à distance autorisées, et connexions à distance autorisées avec certains utilisateurs dont le mot de passe est facile à deviner.
- **Meilleures pratiques :** VA contrôle actuellement 26 règles basées sur la norme ISO 27000, dont des paramètres tels que l'âge minimum du mot de passe et la longueur minimum du mot de passe.
- **Détection des problèmes de configuration de la sécurité :** VA signale chaque problème de configuration, en fournit une description et recommande un plan d'actions pour le corriger.
- **Intégration avec IBM X-Force :** VA extrait des renseignements de sécurité de cinq sources tierces et utilise des critères tels que le vecteur d'attaque, la complexité et la disponibilité d'un correctif connu pour attribuer à chaque vulnérabilité un niveau de gravité. L'échelle des niveaux (critique, élevée, modérée ou faible) aide les administrateurs à comprendre rapidement la gravité des vulnérabilités et à définir les priorités d'action.

Pour corriger une vulnérabilité, VA n'interrompt pas l'exécution de l'image afin d'appliquer un correctif. Il corrige l'image de référence contenue dans le registre, puis déploie une nouvelle instance de cette image dans le conteneur. Cette approche aide à garantir que toutes les instances futures de cette image comporteront le même correctif. En revanche, les machines virtuelles (VM) peuvent toujours être traitées de façon traditionnelle, en utilisant un service de sécurité des nœuds finaux pour corriger les VM et les vulnérabilités de Linux en matière de sécurité.

Ici, on parle Kubernetes

Si vos équipes DevOps utilisent le célèbre logiciel d'orchestration de conteneurs Kubernetes, assurez-vous qu'elle peuvent continuer à utiliser leurs outils favoris. Évaluez également avec quelle facilité une plateforme met à disposition de nouveaux clusters Kubernetes et gèrent les clusters existants.

Interrogez les fournisseurs de plateformes cloud pour savoir s'ils prennent en charge Calico et Istio avec leurs systèmes Kubernetes. Calico et Istio sont deux composants importants de Kubernetes, qui aident à sécuriser les applications et les charges de travail. Calico simplifie la gestion des adresses IP attribuées aux charges de travail sur un nœud de traitement, et programme des listes de contrôle d'accès sur chacun de ces nœuds afin d'appliquer les règles de sécurité. En utilisant les définitions de règles créées et appliquées via des labels de configuration, Istio contrôle à l'aide de certificats les communications entre microservices au sein d'un pod ou d'un cluster Kubernetes.

Créer un système immunitaire de sécurité grâce à une surveillance intelligente

Lorsqu'ils adoptent le cloud, les RSSI s'inquiètent souvent de la faible visibilité et de la perte de contrôle associées. Puisque l'intégralité du cloud d'une entreprise peut devenir inutilisable si une clé spécifique est effacée ou qu'un changement de configuration coupe par inadvertance la connexion avec les ressources sur site ou avec le centre des opérations de sécurité (COS) de l'entreprise, pourquoi les ingénieurs des opérations n'exigeraient-ils pas une visibilité complète sur les charges de travail, les API et les microservices dans le cloud – autrement dit, sur tout ?

Traces d'accès et journaux d'audit

Tous les accès des administrateurs et des utilisateurs, effectués par le fournisseur de cloud ou par votre entreprise, doivent être consignés automatiquement. Un dispositif de suivi de l'activité du cloud peut créer une trace de tous les accès à la plateforme et aux services, y compris les accès effectués par des API, le web et des appareils mobiles. Votre entreprise doit être capable d'exploiter ces journaux et de les intégrer dans son COS.

Veille sécuritaire d'entreprise

Assurez-vous que vous pouvez intégrer tous les journaux et événements dans votre système local de gestion des informations et des événements de sécurité (SIEM) (Figure 3). Certains fournisseurs de services cloud proposent également une surveillance de la sécurité avec gestion et signalement des incidents, une analyse en temps réel des alertes de sécurité et une vue intégrée de vos déploiements hybrides.

IBM QRadar, par exemple, est une solution SIEM complète qui offrent plusieurs solutions de veille sécuritaire capables d'évoluer en fonction des besoins de votre entreprise. Ses fonctionnalités d'apprentissage automatique sont entraînées à partir des modèles de menaces afin de construire un système immunitaire de sécurité prédictif.

Gestion de la sécurité et savoir-faire

Si votre entreprise ne possède pas un savoir-faire important en matière de sécurité, recherchez des fournisseurs capables de gérer la sécurité à votre place. Certains fournisseurs peuvent surveiller vos incidents de sécurité, exploiter des renseignements sur les menaces issus de différents secteurs d'activité et corréler toutes ces informations afin de pouvoir agir en conséquence. Demandez-leur s'ils offrent également un outil unique centralisé qui intègre les services de sécurité internes et gérés.

Enseignement-clé

Le système de sécurité d'une plateforme cloud doit efficacement contrôler les accès, opérer au niveau des charges de travail, suivre l'activité de façon détaillée et s'intégrer avec les systèmes sur site.

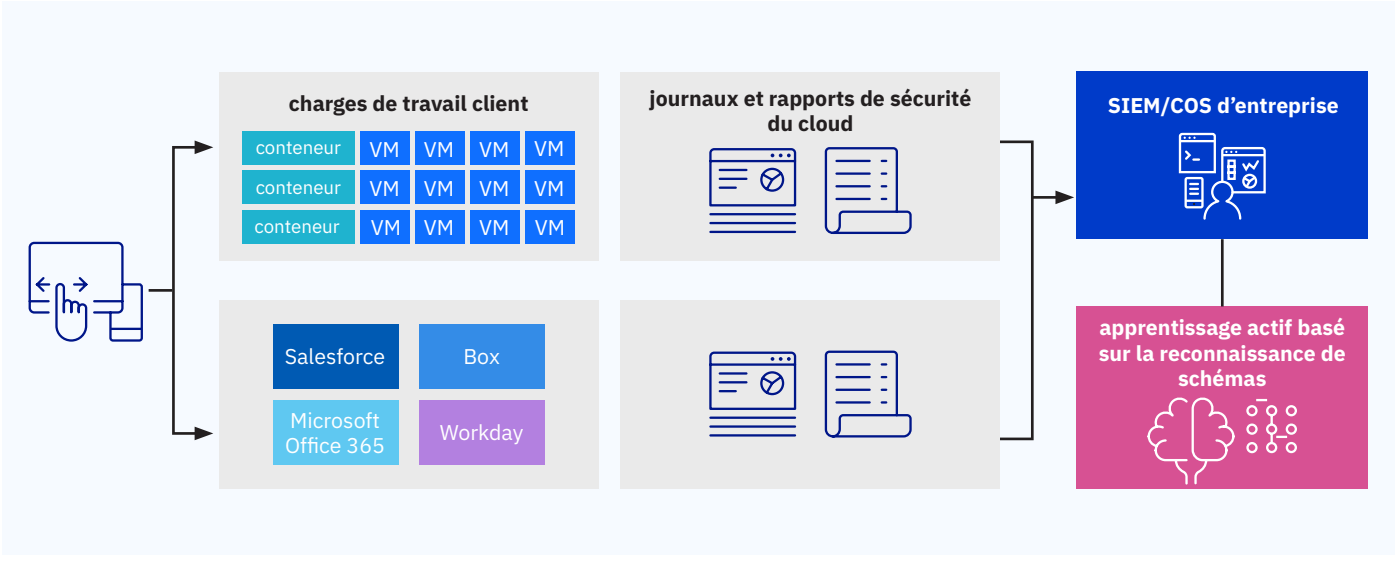


Figure 3. Intégration de la visibilité du cloud dans un SIEM/COS d'entreprise.

Une sécurité qui favorise la réussite de l'entreprise

La technologie du cloud jouant un rôle de plus en plus important dans la gestion d'une entreprise numérique, il est réellement rentable de rechercher un fournisseur de cloud qui offre l'ensemble de fonctionnalités et de contrôles approprié pour protéger vos données, vos applications et l'infrastructure cloud dont dépendent vos applications orientées client. Exigez une solution de sécurisation de plateforme cloud qui couvre les cinq domaines-clés suivants : identité et accès, sécurité du réseau, protection des données, sécurité des applications, visibilité et intelligence. Votre objectif est de moins vous occuper de la technologie et de vous concentrer davantage sur votre cœur de métier.

Un cloud correctement sécurisé offre d'importants avantages métier et informatiques incluant :

- **Production de valeur plus rapide :** La sécurité étant déjà installée et configurée, vos équipes peuvent facilement mettre les ressources à disposition et rapidement prototyper des expériences utilisateur, évaluer les résultats et itérer en fonction des besoins.
- **Investissements moindres :** Utiliser des services de sécurité s'exécutant dans le cloud peut vous éviter de nombreux frais préalables, notamment en ce qui concerne les serveurs, les licences logicielles et les appliances.
- **Charge administrative réduite :** En mettant en place et en gérant une plateforme cloud digne de confiance, un fournisseur proposant des offres de sécurité adaptées supporte la majeure partie de la charge d'administration, ce qui réduit vos coûts de production de rapports et de maintenance des ressources.

Consultez la page web « Gartner peer insights » pour découvrir pourquoi IBM Cloud :

obtient le score le plus élevé pour l'intégration d'entreprise (4,6 étoiles sur 5)

et le score global le plus élevé parmi les principaux fournisseurs de cloud (4,7 étoiles sur 5)

... sur la base de **90 évaluations collectées au cours des 12 derniers mois, en date du 1er juin 2020.**

https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/ibm/product/ibm-cloud

Les évaluations « Gartner peer insights » traduisent les opinions subjectives d'utilisateurs individuels, basées sur leurs propres expériences. Elles ne représentent pas l'opinion de Gartner ou de ses affiliés.

Pour plus d’informations

Pour en savoir plus sur les cinq domaines-clés de la sécurité du cloud et sur les technologies et services IBM associés, consultez la page web : **ibm.com**/cloud/security

Restez connecté

IBM Cloud Blog

Suivez-nous

@IBMcloud

Facebook

Contactez-nous

LinkedIn

YouTube

Compagnie IBM France
17 avenue de l’Europe
92275 Bois-Colombes Cedex

La page d’accueil d’IBM est accessible à l’adresse suivante :
ibm.com

[1] Rapport « Insider Threat 2018 », publié en novembre 2017, http://crowdresearchpartners.com/portfolio/insider-threat-report