Introduction à la sécurité dans le cloud

LIVRE BLANC

Sommaire

Défis de sécurité associés aux différents modèles de cloud 2

Cloud hybride 2

Cloud public 2

Cloud privé 3

L'étape suivante 4

En dépit de la prolifération rapide du cloud computing, il n'existe pas de norme de référence pour le déploiement et l'utilisation des modèles de cloud. Les entreprises utilisent à la fois des clouds publics et privés, et combinent souvent les deux dans un modèle de cloud hybride. Elle déploient des services SaaS (Software-as-a-Service), IaaS (Infrastructure-as-a-Service) et PaaS (Platform-as-a-Service). Certaines équipes informatiques proposent des applications stratégiques dans un seul cloud privé, tandis que d'autres utilisent plusieurs clouds pour les mêmes types d'applications. Certaines valident les projets touchant à l'informatique de l'ombre ou, à l'inverse, les refusent.

Indépendamment du type d'environnement cloud que vous avez choisi, si vous être chargé de superviser ou de déployer des services de cloud dans votre entreprise, une évidence s'impose : quel que soit le degré de complexité de votre déploiement, vous ne pouvez jamais tolérer la compromission de la sécurité de vos données ou de vos applications Si une violation de sécurité ou une cyberattaque compromet vos données ou si des organismes de réglementation mettent en cause votre conformité, il ne sert à rien de pointer du doigt un fournisseur de clouds publics. Au final, c'est à vous d'assumer la responsabilité de votre sécurité, même si le fournisseur de clouds publics possède un modèle de « responsabilité partagée ».

intel Security

TechTarget Custom Media

LIVRE BLANC TECHTARGET

Au vu de la grande variété des déploiements de cloud, qu'est-ce que cela signifie ? Dès lors que les données et les applications transitent par divers types de cloud (privé, public, hybride), comment leur garantir une protection à tout moment ? Lorsque vous utilisez un cloud public, où s'arrête votre responsabilité en matière de sécurité et où commence celle du fournisseur ? Comment s'assurer qu'il n'existe aucune faille dans la protection lorsque les données et applications quittent le périmètre de votre réseau ? À l'heure où les entreprises adoptent les nouvelles technologies de cloud privé, notamment le centre de données défini par logiciel, que faut-il savoir des nouveaux risques encourus ?

Ce livre blanc s'intéresse aux défis de sécurité des différents modèles de cloud. Il propose des recommandations pour éviter de compromettre la protection, indépendamment de la diversité ou de la complexité des modèles de cloud mis en œuvre. Enfin, il fait le point sur certaines technologies essentielles à une sécurité fiable dans l'ère du cloud.

Défis de sécurité associés aux différents modèles de cloud

Quel que soit le degré de complexité de votre déploiement, vous ne pouvez jamais tolérer la compromission de la sécurité de vos données ou de vos applications

On peut affirmer sans crainte de se tromper que le cloud change la donne, surtout en matière de sécurité. Le cloud présente des défis de sécurité bien différents de ceux que nous avons connus jusqu'à présent. Pour les professionnels de la sécurité, il ne s'agit plus simplement de sécuriser le périmètre, de créer une zone démilitarisée (DMZ) ou d'utiliser les dernières solutions antivirus ou antimalware. Il est désormais impératif de posséder une stratégie de sécurité de bout en bout qui garantit une visibilité, des informations, un contrôle et une protection accrus. C'est d'autant plus important que les données et les applications sont constamment déplacées au sein d'environnements toujours plus hétérogènes. Voici les principaux défis posés par chaque modèle de cloud :

Cloud hybride

Le cloud hybride est un environnement de cloud qui utilise une combinaison de services de cloud privé sur site et de services de cloud public tiers, avec des outils d'orchestration entre les deux plates-formes[1]. Les entreprises adoptent de plus en plus les modèles de cloud hybride car ils offrent au département informatique des modèles de déploiement souples. Certaines applications stratégiques peuvent rester sous le contrôle de l'équipe informatique dans un cloud privé. D'autres applications se prêtent mieux aux modèles de cloud public car elles peuvent tirer parti de l'évolutivité, de la réduction de coûts ou de l'activation de ressources en libre-service offertes par ce type de cloud.

Les clouds hybrides présentent des défis très spécifiques, dans la mesure où les données et les applications peuvent transiter vers ou depuis divers environnements cloud : depuis votre centre de données, vers les clouds publics et à nouveau vers votre réseau. Lorsque vos applications et données sont transférées vers l'infrastructure d'un fournisseur de clouds publics, vous risquez de perdre en visibilité et contrôle. Cet aspect du cloud public peut devenir un point d'entrée des logiciels malveillants. Le défi est double. D'une part, il est nécessaire d'étendre la visibilité à toutes les ressources informatiques (sur site et dans le cloud public). D'autre part, il faut implémenter des fonctionnalités cohérentes de surveillance, de protection, de génération de rapports et de correction dans tout l'environnement de cloud hybride.

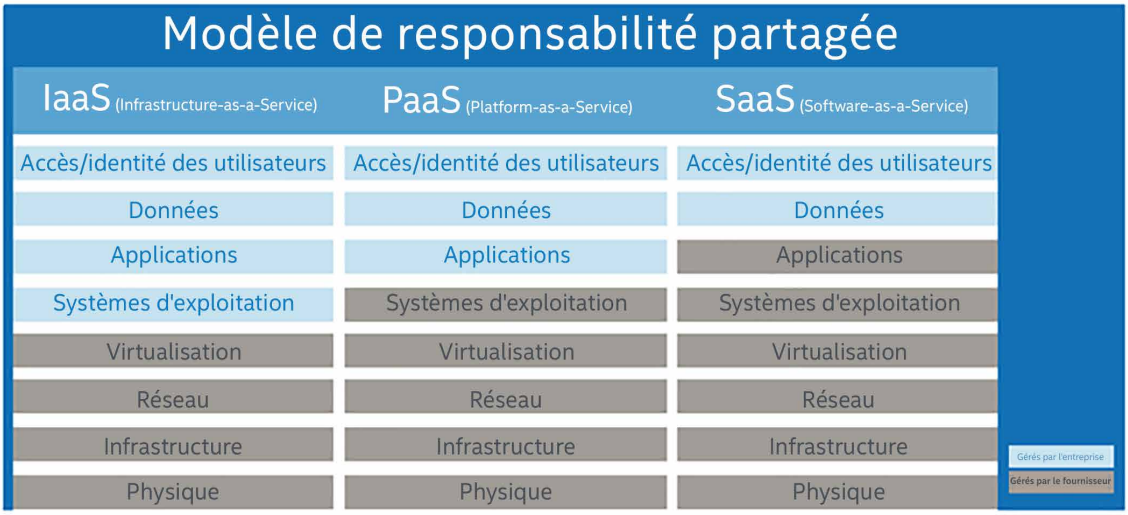
Ce modèle nécessite une stratégie de sécurité de bout en bout capable d'étendre la visibilité et le contrôle. Il doit vous permettre de mettre en œuvre des dispositifs de protection et des stratégies sur l'ensemble des machines virtuelles, où qu'elles soient : dans votre cloud privé ou dans l'infrastructure du fournisseur de cloud public si vous optez pour un environnement de cloud hybride.

Cloud public

Un cloud public est une infrastructure cloud ouverte et accessible au public. Elle est détenue, exploitée et gérée par une société, une université, un organisme public, ou une entité réunissant plusieurs d'entre eux. Il est hébergé sur le site du fournisseur[2]. Du point de vue de la sécurité, le cloud public pose des risques similaires à ceux mentionné pour le cloud hybride. Vous perdez votre visibilité et votre contrôle sur les données et les applications lorsqu'elles sont migrées vers l'infrastructure d'un fournisseur de clouds publics. Vous devez déterminer la part de responsabilité qui revient à votre société et au fournisseur.

Vous ne pouvez pas simplement renoncer à votre responsabilité en matière de sécurité et de conformité et la transférer au fournisseur de clouds publics en supposant qu'il s'en chargera. Il est impératif de connaître le modèle de responsabilité partagée de chaque fournisseur pour chacun des modèles de cloud que vous déployez : SaaS, PaaS et/ou IaaS. La plupart des principaux fournisseurs de clouds publics, notamment Amazon, Google ou Microsoft, décrivent en détail leur modèle de responsabilité partagée sur leur site web. Prenez le temps d'étudier ces modèles et de les appliquer aux divers modèles de déploiement que vous utilisez. Par ailleurs, avant de signer un contrat, vérifiez que les responsabilités sont clairement établies pour chaque scénario et chaque type de service.

Le tableau suivant offre un exemple de modèle de responsabilité partagée applicable au cloud public et répertorie les éléments relevant de la responsabilité de l'entreprise et du fournisseur.



Pour les professionnels de la sécurité, il ne s'agit plus simplement de sécuriser le périmètre, de créer une zone démilitarisée (DMZ) ou d'utiliser les dernières solutions antivirus ou antimalware. Il est désormais impératif de posséder une stratégie de sécurité de bout en bout qui offre une visibilité, des informations, un contrôle et une protection accrus.

L'un des principaux risques de sécurité posés par le cloud public est la facilité de son déploiement. Un chef de service, voire un particulier peut accéder au site d'un fournisseur de cloud public et s'inscrire à un service en quelques clics et à l'aide d'une carte de crédit. Ce type de déploiement qui relève de « l'informatique de l'ombre » peut exposer l'entreprise à des risques de sécurité accrus. Il se peut que l'équipe informatique n'en soit même pas informée et que l'utilisateur ne soit pas au courant des types de contrôles de sécurité à mettre en œuvre pour préserver la sécurité de l'entreprise.

L'un des grands défis du cloud public consiste à savoir qui dans l'entreprise utilise les services de cloud public, quels types de services sont déployés (SaaS, PaaS et/ou IaaS) et enfin comment et quand ces services sont utilisés. Une fois en possession de ces informations, vous avez besoin de solutions technologiques qui vous permettent de garder un certain contrôle, les solutions variant selon le type de services utilisés. Si l'on se réfère au modèle de responsabilité partagée, il est clair que l'accès, le contrôle des identités et la protection des données sont des aspects prioritaires de la sécurité du cloud, surtout dans le cas des services SaaS. Quant aux environnements IaaS, ils nécessitent une solution de sécurité capable de surveiller et de contrôler l'intégrité des fichiers, d'interdire l'installation des logiciels non autorisés et de surveiller toutes les modifications apportées. En outre, votre choix doit se porter sur une solution qui offre une visibilité au niveau de l'hôte afin de pouvoir surveiller toutes vos applications.

Cloud privé

Un cloud privé offre des avantages similaires à ceux du cloud public, y compris l'évolutivité et l'activation des ressources en libre-service, si ce n'est qu'il est déployé au sein d'une architecture propriétaire. À la différence des clouds publics qui offrent des services à plusieurs entreprises ou organisations, un cloud privé est dédié à une seule[3].

Vous ne pouvez pas simplement renoncer à votre responsabilité en matière de sécurité et de conformité et la transférer au fournisseur de clouds publics.

Un cloud privé permet de garder les données et applications sous le contrôle de l'organisation. En d'autres termes, celles-ci ne quittent pas votre périmètre pour être déplacées vers l'infrastructure d'un autre fournisseur. De prime abord, on pourrait penser que la mise en œuvre de la sécurité est dès lors bien plus simple que dans les déploiements de cloud public ou hybride. Si c'est effectivement le cas à certains égards, le cloud change néanmoins la donne.

Les clouds privés nécessitent l'adoption de nouveaux modèles de déploiements pour les centres de données. Ceux-ci doivent étendre la virtualisation à toute l'infrastructure et permettre aux entreprises d'utiliser les fonctionnalités de cloud, à savoir la mise en commun des ressources, l'évolutivité, les fonctions en libre service et la refacturation. L'entreprise peut ainsi bénéficier d'un modèle informatique davantage axé sur les services. Toutefois, ce modèle peut induire de nouveaux risques de sécurité que l'entreprise doit anticiper et prendre en compte dans sa stratégie.

Voici un exemple. Lorsque vous étendez la virtualisation aux réseaux et au stockage en plus des serveurs du centre de données, le volume de trafic bidirectionnel entre les machines virtuelles augmente sensiblement. Les anciennes technologies axées sur la sécurisation du périmètre n'auront aucune visibilité sur ce trafic et ne seront pas en mesure de le protéger. Vous devez avoir la possibilité d'appliquer des contrôles de sécurité intégrant l'inspection approfondie des paquets pour tout le trafic entre machines virtuelles.

Prenons un autre exemple : le déploiement de nouvelles machines virtuelles peut entraîner l'apparition de failles de sécurité si vos stratégies et vos mécanismes de protection ne sont pas immédiatement appliqués à celles-ci. Une telle situation est évidemment inacceptable. Dès lors, vous devez chercher à implémenter,

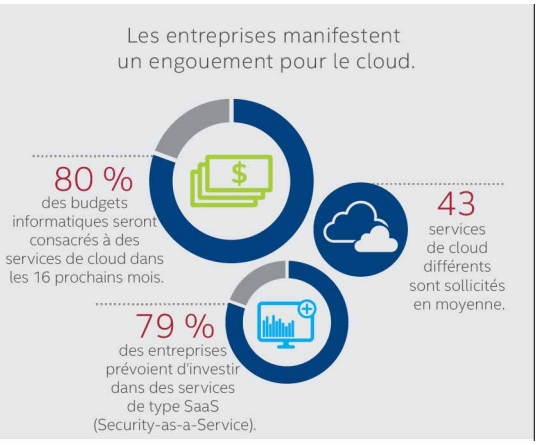
Les solutions de sécurité doivent être intégrées à l'environnement informatique global, pas ajoutées a posteriori. Les équipes informatiques et de sécurité doivent utiliser des outils et des technologies spécialement conçus pour répondre aux défis du cloud.

dans le cloud privé, une sécurité basée sur un modèle virtualisé ou défini par logiciel qui tire parti de l'automatisation et de l'orchestration des stratégies de sécurité. Vous limitez ainsi le temps et les risques associés au déploiement et à l'activation manuels. Si et quand une machine virtuelle est déplacée, tous les paramètres de sécurité et les dispositifs de protection doivent idéalement migrer avec celle-ci.

Autre exemple : la nature dynamique de l'activation des machines virtuelles et de leur charge globale sur les serveurs dans un environnement de cloud privé peut compliquer la planification de la capacité. Si vous exécutez une solution antivirus qui n'a pas été conçue pour les environnements virtuels d'un cloud privé, la tâche peut être quasi irréalisable. Même si une solution antivirus traditionnelle est exécutée sur ces machines virtuelles, l'impact cumulé sur les performances de l'infrastructure est parfois très élevé. Cet impact aura aussi une incidence directe sur le nombre de machines virtuelles qu'il est possible d'exécuter sur un serveur et, donc, sur la proportion prévue de machines virtuelles par serveur et sur le rendement opérationnel. Une solution antivirus optimisée pour la virtualisation sera plus efficace pour protéger cet environnement élastique sans nuire aux performances et à l'évolutivité.

L'étape suivante

L'évolution vers le cloud est l'une des tendances informatiques majeures de notre époque. Comme l'a dit IDC, « le cloud avant tout » est en passe de devenir le nouveau leitmotiv des départements informatiques en entreprise[4]. D'après le récent rapport sur l'adoption du cloud d'Intel Security, 80 % des budgets informatiques iront aux services de cloud au cours des 16 prochains mois et 96 % des entreprises augmenteront leurs investissements dans les technologies de cloud[5]. En outre, le rapport révèle que les sociétés utilisent en moyenne 43 services de cloud différents et 40 % d'entre elles traitent ou stockent déjà des données sensibles dans le cloud. Par ailleurs, si 77 % des entreprises interrogées déclarent avoir plus confiance dans le cloud qu'il y a un an, 66 % sont également d'avis que la direction ne comprend pas totalement les risques associés au stockage des données sensibles dans le cloud.



Pour les professionnels de la sécurité, l'adoption du cloud nécessite une nouvelle approche. Tout le défi de la protection du cloud consiste à intégrer les solutions de sécurité à l'environnement informatique global dès le départ, pas ajoutées a posteriori. Les équipes informatiques et de sécurité doivent utiliser des outils et des technologies spécialement conçus pour répondre aux défis du cloud. Enfin, ces outils et technologies doivent être mis en œuvre dans le cadre d'un modèle de déploiement intégré. La protection doit être implémentée de façon uniforme et cohérente dans tous les environnements de cloud. Les fonctionnalités, dont la détection des menaces et la prévention des intrusions, doivent être fournies en temps réel pour protéger à tout moment toute l'organisation, quel que soit l'emplacement des données et des applications.

Lorsque vous concevez votre stratégie de sécurité du cloud, il est important de faire appel à un fournisseur qui propose un modèle intégré de sécurité du cloud, ainsi qu'un large éventail de solutions conçues pour le cloud. Parmi les technologies indispensables, citons un contrôleur de sécurité défini par logiciel, une plate-forme de sécurisation du réseau virtuelle, une protection antimalware virtuelle, une protection du cloud public basée sur l'hôte, un système avancé de cyberveille sur les menaces et la gestion centralisée. Ces solutions étroitement intégrées constitueront la base de votre stratégie de sécurité du cloud actuelle et future. Et, comme c'est souvent le cas pour l'informatique d'entreprise, l'avenir est à nos portes.

Si vous êtes prêt à passer à l'étape suivante pour protéger votre environnement de cloud, n'hésitez pas à contacter Intel Security à l'adresse suivante : **www.mcafee.com/fr/solutions/secure-cloud/index.aspx**.

1 « Hybrid Cloud » (Le cloud hybride), SearchCloudComputing, TechTarget

2 « The NIST Definition of Cloud Computing » (Le cloud tel que défini par le NIST), Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, septembre 2011

3 « Private Cloud » (Le cloud privé), SearchCloudComputing, TechTarget

4 « IDC Predicts the Emergence of 'the DX Economy' in a Critical Period of Widespread Digital Transformation and Massive Scale Up of 3rd Platform Technologies in Every Industry » (IDC prédit l'émergence de l'économie de transformation numérique [DX] dans le cadre d'une période critique de transformation numérique étendue et d'extension massive des technologies de la 3e plate-forme dans tous les secteurs), IDC, 4 novembre 2015

5 « Ciel dégagé à l'horizon ? Le point sur l'adoption du cloud », Intel Security, avril 2016

Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com