MEILLEURES PRATIQUES DE SÉCURITÉ POUR LES ENVIRONNEMENTS DE CLOUD

Stratecast | FROST & SULLIVAN

Note d'information sponsorisée par IBM

Michael Suby
Vice-président de la recherche, Stratecast

Juillet 2014

INTRODUCTION

Le cloud ne va cesser de se développer pour finalement devenir une composante essentielle de votre environnement informatique. Cette évolution est inévitable, et encore plus si l'on prend en compte les éléments suivants :

- **Attrait économique** : l'attrait économique des services d'infrastructure cloud (par exemple, l'infrastructure sous forme de service, ou IaaS) augmente à chaque nouvelle offensive lancée dans le cadre de la guerre des prix. Attirée par cet aspect économique, votre organisation sera-t-elle confrontée à l'escalade de la protection des données, des risques opérationnels, de la complexité de la gestion et de l'incertitude liée à la conformité ?
- **Tendance au libre-service** : comme l'a révélé une enquête Frost & Sullivan réalisée en fin 2013, 70 % des utilisateurs finaux ignorent les procédures d'approbation informatique et souscrivent à des services cloud non vérifiés, pour différentes raisons, notamment la poursuite de leurs objectifs commerciaux, l'amélioration de leur productivité ou encore pour favoriser l'innovation. Votre organisation peut-elle atténuer les risques de sécurité associés à une utilisation non contrôlée et invisible des logiciels sous forme de service (SaaS) ?
- **Opportunités associées à l'Internet des objets** : l'apogée de l'Internet des objets est toute proche, tout comme la possibilité d'envoyer et de collecter des flux de données rudimentaires n'est plus une contrainte technologique. De la même manière, l'extraction d'informations exploitables de ces montagnes de données n'est plus une potentialité, mais bien une réalité rendue possible par l'élasticité du cloud. Préparer votre organisation à prendre et surfer sur les vagues de l'Internet des objets et des Big Data et de l'analyse ne peut plus attendre... Mais êtes-vous prêt à relever le défi de la sécurité des informations qu'implique l'utilisation du cloud ?

La réponse à ces questions tient en quelques mots : la gestion proactive et intelligente des risques. Alors même que la technologie de l'information évolue à toute vitesse et de manière relativement imprévisible, une approche globale de la gestion des risques adaptable et flexible aide les organisations à adopter les services cloud sans craindre pour la sécurité de leurs informations.

Ainsi, ce document a pour objectif de présenter une approche directe de la sécurité du cloud. La base même de cette approche vous aidera non seulement à atténuer les risques liés aux déploiements et à l'utilisation du cloud, mais également à améliorer et normaliser votre conception de la sécurité et vos pratiques associées dans tous vos environnements, aussi bien sur les clouds publics et privés que sur les serveurs bare metal. En outre, cette approche vous permettra également d'éviter les futures réorganisations en matière de sécurité qui pourraient vous échoir suite à l'émergence de nouvelles technologies de l'information et autres menaces de sécurité.

RISQUE DE SÉCURITÉ CROISSANT ASSOCIÉ AU CLOUD

Le cloud et ses technologies sous-jacentes offrent de nombreux avantages. Toutefois, sans une compréhension profonde des risques de sécurité et des menaces qui les sous-tendent, mais aussi de leurs différences selon le modèle de cloud utilisé, ces avantages perdent de leur intérêt, et de graves conséquences peuvent survenir, notamment une interruption des opérations, une violation des données, un vol de propriété intellectuelle, une violation de conformité ou encore une atteinte à l'image de marque.

En outre, les coûts directs et indirects qu'engendrent toutes ces conséquences et les restrictions que cela implique neutralisent les avantages escomptés de l'adoption du cloud.

Le cloud et ses technologies sous-jacentes offrent de nombreux avantages. Toutefois, sans une compréhension profonde des risques de sécurité et des menaces qui les sous-tendent, mais aussi de leurs différences selon le modèle de cloud utilisé, ces avantages perdent de leur intérêt, et de graves conséquences peuvent survenir.

Si on la compare aux centres de données privés sur site (c'est-à-dire l'environnement traditionnel),[1] l'utilisation du cloud implique un risque croissant. Mais comme nous le suggérons ici, cette escalade des risques peut parfaitement être contrôlée. Aussi les risques associés au cloud peuvent-ils être atténués et ses avantages être exploités. En substance, pour utiliser le cloud en toute sécurité, il suffit de poursuivre les mêmes objectifs que ceux fixés dans le cadre d'un environnement traditionnel.

Objectifs de sécurité d'un environnement traditionnel

- **Protégez-vous contre les cybermenaces** : défendez-vous face aux menaces provenant d'Internet et de dispositifs de confiance pourtant compromis.
- **Minimisez vos vulnérabilités** : réduisez le champ d'attaque en limitant les vulnérabilités exploitables sur l'ensemble de votre pile logicielle et de vos flux de données.
- **Protégez vos données** : isolez et protégez vos données importantes tout au long de leur cycle de vie (qu'elles soient en cours d'utilisation, au repos, en transit ou archivées).
- **Contrôlez vos opérations** : faites en sorte que la surveillance et la visibilité de vos opérations informatiques et de sécurité, ainsi que les processus manuels, soient toujours efficaces et conformes aux normes sectorielles et aux réglementations gouvernementales.

Trois types de cloud

Pour bien évaluer les risques croissants associés au cloud, il est nécessaire de comprendre que les risques diffèrent en fonction du type de cloud utilisé. D'une manière générale, le modèle de cloud, qui comprend différents types de cloud, consiste en une approche de la configuration, du provisionnement et de la gestion d'une infrastructure de centre de données et d'applications. Chaque cloud utilise l'automatisation, la normalisation et la virtualisation pour affecter les ressources informatiques de manière efficace et optimale. Au-delà de ces similitudes, les trois types de cloud existants présentent des différences notables :

[1] L'infrastructure sur site inclut des centres de données utilisés en tant que nœuds sur le réseau local (LAN) ou le réseau étendu (WAN) de l'organisation. Dans tous les cas, le centre de données fait partie intégrante d'un réseau privé dédié.

- **Cloud privé** : dans cet environnement de cloud, l'infrastructure de serveur virtuel est dédiée à une seule et même entreprise. L'environnement dédié (parfois appelé « cloud privé virtuel ») peut être hébergé dans le centre de données d'un fournisseur de cloud, ce qui permet alors à l'entreprise de bénéficier de la confidentialité qu'offre un environnement dédié sans avoir à investir dans un centre de données. Le cloud privé peut également être hébergé dans le centre de données de l'entreprise.
- **Cloud public** : dans cet environnement informatique partagé, l'infrastructure est hébergée dans le centre de données d'un fournisseur de services cloud. Le fournisseur de services cloud fournit aux utilisateurs des capacités de stockage et informatiques à la demande via des portails en libre-service, et les utilisateurs paient la capacité qu'ils utilisent.
- **Cloud hybride** : cet environnement permet aux entreprises de configurer et gérer différents environnements de cloud (publics ou privés, sur site ou hébergés) de manière centralisée via une console de gestion commune.

Risque croissant des clouds

- **Le modèle de cloud public repose sur le principe de mutualisation**, ce qui offre l'avantage de réduire les coûts des locataires individuels. Toutefois, la mutualisation augmente également le risque potentiel de cyberattaque en provenance de l'extérieur comme de l'intérieur. Sur le plan extérieur, un fournisseur de cloud public est une cible importante et intéressante, car il regroupe plusieurs locataires, qui eux-mêmes constituent des cibles potentielles. Une fois l'offre souscrite, chaque locataire devient une victime potentielle. Du point de vue intérieur, un acteur malveillant peut également être un utilisateur ayant décidé de monter des attaques contre ses colocataires afin de les espionner. Paradoxalement, l'élasticité du cloud ne se limite pas aux seuls utilisateurs légitimes. Les acteurs malveillants peuvent également exploiter cette élasticité pour réaliser leurs méfaits ; par exemple, ils peuvent l'utiliser pour créer une armée de botnets dynamiques qui pourra obliger le fournisseur de cloud à prendre des mesures pour stopper l'attaque, affectant par la même occasion ses prestations auprès des autres locataires.

- **La responsabilité de la sécurité est partagée** ; contrairement aux environnements traditionnels, qui se fondent sur le principe de la propriété unique et de l'exploitation par une seule et même entité, dans les trois modèles courants de cloud public, à savoir l'infrastructure sous forme de service (IaaS), la plateforme sous forme de service (PaaS) et le logiciel sous forme de service (SaaS), le fournisseur de cloud et ses abonnés (les locataires) se partagent la responsabilité de la sécurité. Toutefois, le niveau de responsabilité incombant au fournisseur de cloud varie en fonction du modèle utilisé (IaaS, PaaS ou SaaS) (voir le tableau disponible à la page suivante). De la même manière, la visibilité sur les opérations de sécurité du fournisseur de cloud n'est pas aussi bonne et déterministe que dans les environnements traditionnels. Par conséquent, les locataires sont indirectement invités à faire confiance au fournisseur sans pouvoir vérifier quoi que ce soit. Par exemple, l'analyse et la résolution des vulnérabilités sont certaines des responsabilités de sécurité assumées par le fournisseur de cloud (par exemple, dans le cadre des interfaces de réseau virtuel et de l'hyperviseur dans le modèle IaaS, jusqu'au logiciel d'application dans le modèle SaaS) ; mais la fréquence et le degré d'analyse des vulnérabilités, ainsi que le niveau de priorité des résolutions sont déterminés par le fournisseur de cloud, et non par les locataires individuels. De la même manière, l'identification et l'atténuation des incidents de sécurité et des erreurs de configuration imputables aux couches de l'infrastructure de cloud du fournisseur de cloud ne sont pas du ressort des locataires. Dans les environnements de cloud, la force de la sécurité dépend en partie de la force des opérations de sécurité et de l'approche de gestion appliquée par le fournisseur de cloud.

> Dans les environnements de cloud, la force de la sécurité dépend en partie de la force des opérations de sécurité et de l'approche de gestion appliquée par le fournisseur de cloud.

Responsabilités de sécurité partagées

Couche cloud	Environnements traditionnels	Modèles de cloud		
		IaaS	PaaS	SaaS
Données		Responsabilité incombant au locataire de cloud		
Interfaces (API, interfaces utilisateur graphiques)				
Applications				
Pile de solutions (langues de programmation)				
Système d'exploitation (SE)	Entièrement détenus et exploités en interne			
Machines virtuelles				
Interfaces de réseau virtuel				
Hyperviseurs		Responsabilité incombant au fournisseur de cloud		
Mémoire et traitement				
Stockage des données (disques durs, disques amovibles, sauvegardes, etc.)				
Réseau (interfaces et périphériques, infrastructure des communications)				
Installations physiques / centres de données				

Source : PCI Security Standards Council, « Information Supplement: PCI DSS Cloud Computing Guidelines » (février 2013) et Stratecast

- **Mobilité des charges de travail** : également liée à la proposition de valeur à moindre coût du cloud public, nous retrouvons la mobilité des charges de travail virtuelles sur les serveurs physiques et centres de données du fournisseur de cloud, qui permet d'optimiser l'infrastructure. Néanmoins, et contrairement à une charge de travail hébergée sur un serveur dédié, dans le cadre duquel ladite charge de travail est protégée par un ensemble de couches de protection, il est plus difficile d'assurer une telle protection lorsque les charges de travail virtuelles sont déplacées. Ces couches de sécurité doivent être tout aussi mobiles que les charges de travail virtuelles, et ce sans impliquer une quelconque perte d'intégrité.
- **Tous les utilisateurs sont distants** : un autre avantage du cloud public, mais qui présente un risque élevé en termes de sécurité, consiste en ce que tous les utilisateurs sont distants. Bien que l'accès soit universel et adapté à tous les types de dispositifs, à l'inverse des modèles de cloud dont l'accès est limité aux seuls dispositifs et utilisateurs basés dans les locaux de l'entreprise, les procédures de validation utilisateur requises (par exemple, une carte d'accès au site, un mot de passe d'accès LAN ou encore un ID de dispositif enregistré) ne sont pas toujours

mises en place. Par conséquent, le flux de données circulant « dans la nature » court un risque plus grand sur un cloud public. En outre, l'utilisation accrue du modèle SaaS augmente les risques en raison de l'éparpillement des données d'identification et des mécanismes d'adaptation utilisés par les utilisateurs (par exemple, utilisation répétée de mots de passe faciles à retenir) et des problèmes soulevés par la gestion des comptes (par exemple, annulation de l'accès à plusieurs services SaaS suite au départ d'un employé).

APPROCHE POUR UN CLOUD SÉCURISÉ

L'évolution continue des menaces de sécurité et l'adoption par les organisations de nouvelles technologies de l'information ont été sources d'innovations en matière de sécurité. La sécurité a évolué de pair avec les menaces et l'informatique, soit en s'adaptant, soit via le développement de nouvelles catégories et pratiques de sécurité. Les technologies de sécurité et leurs concepts de base déjà appliqués dans les environnements traditionnels peuvent être adaptés au cloud, ce qui constitue un véritable avantage pour sa sécurisation. Mais cela ne signifie pas pour autant que le cloud peut être sécurisé de manière simple grâce à la portabilité des technologies de sécurité utilisées dans les environnements traditionnels. En vérité, même si les préceptes fondamentaux permettent de sécuriser le cloud de manière efficace, une compréhension approfondie des risques croissants et du caractère unique du cloud est nécessaire pour les mettre en œuvre.

Les technologies de sécurité et leurs concepts de base déjà appliqués dans les environnements traditionnels peuvent être adaptés au cloud, ce qui constitue un véritable avantage pour sa sécurisation. Mais cela ne signifie pas pour autant que le cloud peut être sécurisé de manière simple grâce à la portabilité des technologies de sécurité utilisées dans les environnements traditionnels.

En outre, comme nous le verrons plus tard, les utilisateurs du cloud ont toujours plus de choix, notamment en ce qui concerne le modèle IaaS. Le choix étant particulièrement vaste dans ce domaine, les utilisateurs peuvent combiner, pour des résultats optimaux, performances, confidentialité et prix pour chacune de leurs charges de travail. Les options possibles incluent notamment le cloud public (serveur virtuel, connexion à un réseau public), le cloud privé (serveur virtuel, connexion à un réseau privé) ou encore le cloud bare metal (serveur dédié, connexion à un réseau privé).

Les principaux concepts et technologies de sécurité requis pour sécuriser les environnements de cloud incluent ce qui suit :

- **Segmentation et isolement** : l'aspect mutualisé du cloud public requiert des organisations qu'elles établissent et gèrent des murs virtuels autour de chaque charge de travail et du trafic réseau circulant entre les charges de travail et de l'une à l'autre. Cet effort est primordial pour protéger les charges de travail et les données des autres locataires et administrateurs du cloud, et, du point de vue de la performance, pour s'assurer que la charge de travail n'est pas privée de ses ressources réseau, informatiques et de stockage. Selon la charge de travail, l'approche de la performance « au mieux » n'est pas acceptable, et il est nécessaire de mettre en place des accords de niveau de service (SLA) vérifiables.
- **Détection et atténuation des menaces** : les menaces visant à perturber les opérations, compromettre l'intégrité ou préparer le terrain en vue d'une exfiltration des données sont omniprésentes. Les fournisseurs de cloud l'ont bien compris et ont développé des technologies de détection et d'atténuation des menaces et intégré des procédures à leurs opérations afin de mieux servir

l'ensemble de leurs locataires, et bien évidemment, de maintenir la disponibilité et l'intégrité du service. Malgré tout, les menaces avancées étant micro-ciblées, les efforts de détection des menaces déployés par les fournisseurs de cloud sont loin d'être la panacée. Il est donc recommandé à tous les locataires de cloud d'ajouter une couche de détection des menaces supplémentaire pour se défendre contre les menaces extérieures ayant réussi à franchir la barrière générale de détection des menaces installée par le fournisseur de cloud.

- **Informations sur la sécurité et gestion des événements (SIEM)/Gestion des journaux** : aucune défense n'est et ne sera jamais impénétrable ; il est donc nécessaire d'installer un filet de sécurité et de recueillir en permanence les données afin de repérer les signes avant-coureurs de toute attaque en plusieurs étapes. Poursuivant dans la même veine que dans les environnements traditionnels, les procédures SIEM et de gestion des journaux nouvelle génération s'imposent comme LE filet de sécurité des environnements de cloud. Pour une efficacité optimale, la collecte de données doit être la plus étendue possible, de la couche de réseau jusqu'à la couche d'application ; la surveillance doit se dérouler en temps réel et générer des résultats qui puissent être analysés en fonction du contexte. Si une approche hybride (c'est-à-dire une combinaison de centre de données privé (environnement traditionnel) et de cloud public) est utilisée, les fonctions SIEM et de gestion des journaux doivent être appliquées de manière homogène sur les deux environnements. En outre, la sécurité intelligente doit prendre en compte les facteurs externes comme internes afin de filtrer les énormes quantités de problèmes de sécurité quotidiens et se concentrer sur une poignée de problèmes prioritaires plus faciles à gérer.
- **Réponse aux incidents et analyse** : malgré tous les efforts déployés pour protéger les charges de travail virtuelles hébergées dans les environnements de cloud, l'éventualité d'un incident de sécurité majeur n'est pas à écarter et doit être gérée avec toute la rationalité et la prudence qui s'imposent. Aussi une planification et des répétitions permettront-elles de garder la tête froide dans les moments critiques. Également essentielle, l'analyse permet quant à elle de mesurer l'étendue de la menace et, tout aussi important, d'apporter les ajustements nécessaires pour resserrer la défense. Des fonctions SIEM et de gestion des journaux complètes sont essentielles à la bonne exécution de l'analyse et la réponse aux incidents.
- **Gestion des identités et des accès** : comme nous l'avons déjà expliqué, la distance (c'est-à-dire l'accès universel et à partir d'un dispositif quel qu'il soit) des services de cloud public et la multitude d'abonnements SaaS accentuent le besoin de mettre en place un système de gestion des identités et des accès pour contrôler les droits d'accès des utilisateurs dans les environnements privés et publics. Les fonctions de gestion automatique des abonnements (inscriptions SaaS en masse, gestion des mots de passe en libre-service et révocation des droits d'accès des employés ayant quitté l'entreprise dans l'ensemble des environnements) sont également importantes. Autre fonction de gestion des identités et des accès, la création de rapports relatifs aux activités de connexion des utilisateurs permet de repérer les activités douteuses des utilisateurs et autres administrateurs et d'affecter les coûts des services cloud à chaque individu et service. Enfin, l'authentification unique permet quant à elle de lutter contre l'éparpillement des données d'identification, et représente un gain de temps. En effet, les utilisateurs ne perdent plus leur temps à réinitialiser leurs mots de passe oubliés, ni à se connecter aux abonnements SaaS de manière individuelle.
- **Protection des données** : les violations de données sont un phénomène courant, souvent relayé par les médias ; mais de toute évidence, bon nombre de cas restent encore indétectés ou ne sont pas ouvertement signalés. Différentes approches coordonnées permettent d'atténuer le risque de violation de données (par exemple, la segmentation et l'isolement, l'analyse des vulnérabilités, les informations sur la sécurité et la gestion des événements ou encore la gestion des identités et des accès). Il est important de chiffrer les

données critiques, et ce à tous les stades de leur cycle de vie (au repos, en transit ou en cours d'utilisation). En outre, les clés de chiffrement de tout utilisateur de cloud doivent être inaccessibles au fournisseur de cloud, ceci afin d'éviter qu'il accède aux données des locataires, et de manière à garantir la totale suppression des données sur le cloud (en détruisant les clés de chiffrement).

- **Développement sécurisé de logiciels** : les professionnels de la sécurité considèrent le développement sécurisé de logiciels comme essentiel, car il permet de réduire de manière systématique la fréquence et la gravité des vulnérabilités logicielles. Au vu de l'exposition accrue, le développement sécurisé de logiciels s'avère particulièrement important dans les environnements de cloud public.

- **Analyse des vulnérabilités et gestion des correctifs** : même en mettant tous les efforts au service du développement sécurisé de logiciels, les logiciels restent vulnérables, ceci pour la simple et bonne raison que les auteurs de menaces continuent de mettre au point des techniques toujours plus sophistiquées. En outre, d'autres couches logicielles sous-jacentes (par exemple, les systèmes d'exploitation) ou parallèles aux applications (par exemple, les navigateurs, les pilotes et les lecteurs) peuvent présenter des vulnérabilités. Aussi une bonne pratique consiste-t-elle à analyser les vulnérabilités et à gérer les correctifs régulièrement ; les vulnérabilités dans la configuration d'une charge de travail virtuelle étant conservées à chaque nouvelle instance de cette même charge de travail, et ce jusqu'à ce qu'elles soient détectées et totalement supprimées du profil de configuration, cette pratique s'avère particulièrement importante.

BIEN CHOISIR SES TECHNOLOGIES DE SÉCURITÉ

Bien que les individus et les processus participent largement aux efforts de sécurité, la technologie est également un facteur essentiel. L'efficacité de la sécurité ne pourra être que fragilisée si vous combinez à une équipe de sécurité de haut vol et à des processus éprouvés des technologies de qualité inférieure. C'est pourquoi nous recommandons le sous-ensemble d'attributs ci-dessous, qui selon nous représente les technologies de sécurité les plus efficaces pour tout environnement de cloud. Considérant que la sécurité du cloud implique un risque supplémentaire, nous avons séparé les attributs de technologie de sécurité en deux catégories distinctes, à savoir (1) les attributs optimisés pour les entreprises et (2) ceux optimisés pour le cloud. Bien qu'ils ne s'excluent pas mutuellement (en effet, les attributs optimisés pour le cloud sont compatibles avec les environnements traditionnels et inversement), les attributs optimisés pour le cloud reflètent des fonctions avancées nécessaires aux environnements de cloud, les organisations ne cessant d'aller de l'avant et de pousser leur utilisation des services cloud en passant des simples tests et tactiques aux utilisations de routine et stratégies.

“Bien que les individus et les processus participent largement aux efforts de sécurité, la technologie est également un facteur essentiel. L'efficacité de la sécurité ne pourra être que fragilisée si vous combinez à une équipe de sécurité de haut vol et à des processus éprouvés des technologies de qualité inférieure.”

Attributs optimisés pour les entreprises

- **Meilleur de sa catégorie** : dans l'hypothèse raisonnable où les quelques technologies de sécurité présentent des fonctions de sécurité similaires, cet attribut couvre d'autres caractéristiques comparatives, telles que la performance (configuration BITW (Bump In The Wire)), la modularité, l'interopérabilité et l'administration efficace. L'attribut « Meilleur de sa catégorie » prend également en compte la stabilité de

l'entreprise du fournisseur, son engagement vis-à-vis de la recherche et du développement et son support client.

- **Respect de la conformité** : le respect des réglementations, notamment les lois relatives au contrôle des données, prend de l'ampleur. Alléger le fardeau qu'implique de justifier sa conformité et limiter la longueur et la gravité des instances de non-conformité font également partie des attributs optimisés pour les entreprises.
- **Administration basée sur les unités et les rôles** : les services d'entreprise (par exemple, Finances, Ressources humaines ou Juridique) sont des exemples d'unités distinctes d'une organisation globale qui souhaitent ou ont besoin d'exercer un contrôle administratif autonome sur leurs propres politiques de sécurité. Parce qu'elle applique la meilleure pratique des « droits d'accès minimum », l'administration basée sur les rôles est également requise dans les technologies de sécurité optimisées pour les entreprises.

Attributs optimisés pour le cloud

- **Déployable rapidement et hautement automatisé**, telles sont les caractéristiques clés des services cloud. Lorsque vous développez la sécurité autour de chaque charge de travail virtuelle et chaque flux de réseau, il est essentiel de remplir ces conditions de manière à favoriser l'adoption des services cloud.
- **Extensibilité d'un écran unique** : l'utilisation d'interfaces d'administration distinctes pour les environnements traditionnels et de cloud entraîne une fragmentation des politiques de sécurité, une incertitude sur le plan de la conformité et une inefficacité des opérations de sécurité. En outre, sans l'extensibilité d'un écran unique, la flexibilité de déplacement des charges de travail entre les environnements traditionnels et les environnements de cloud est entravée. Par conséquent, il est fortement souhaitable de mettre en place une interface d'administration inter-environnements.
- **Adaptable** : tout comme la part de responsabilités des fournisseurs de cloud en matière de sécurité varie selon le modèle de cloud utilisé, les opérations et pratiques de sécurité appliquées par les fournisseurs de cloud au sein d'un même modèle de cloud diffèrent également. Idéalement, les variations de niveau d'attention fourni par chaque fournisseur de cloud en matière de sécurité et les méthodes utilisées pour vérifier ce niveau d'attention sont connues ; ainsi, lorsqu'une charge de travail est placée dans l'environnement d'un fournisseur de cloud, la responsabilité assumée par les locataires est définie de manière précise. En d'autres termes, la sécurité des locataires s'adapte automatiquement et sans heurt aux conditions de l'environnement et au contexte de la charge de travail (par exemple, la charge de travail contient des données sensibles ou une opération stratégique ou au contraire, des données peu importantes pour les pirates informatiques ; ou les fluctuations de performances, dans la limite du raisonnable, sont tolérées). Cette adaptabilité permet aux organisations de choisir leurs fournisseurs de cloud en toute discrétion, et de décider, une fois encore à leur entière discrétion, quelles charges de travail elles souhaitent migrer vers le cloud.

IBM RELÈVE LES DÉFIS LIÉS À LA SÉCURITÉ DU CLOUD DEPUIS LE DÉBUT

La sécurité du cloud peut être établie et obtenue de manière efficace, mais pas par le fruit du hasard ; la planification est primordiale. Il ne faut pas voir en la relative nouveauté du cloud et en ses défis uniques la possibilité d'apprendre « sur le tas » ; bien au contraire, il faut savoir se préparer dès le départ et faire montre d'une expertise exceptionnelle.

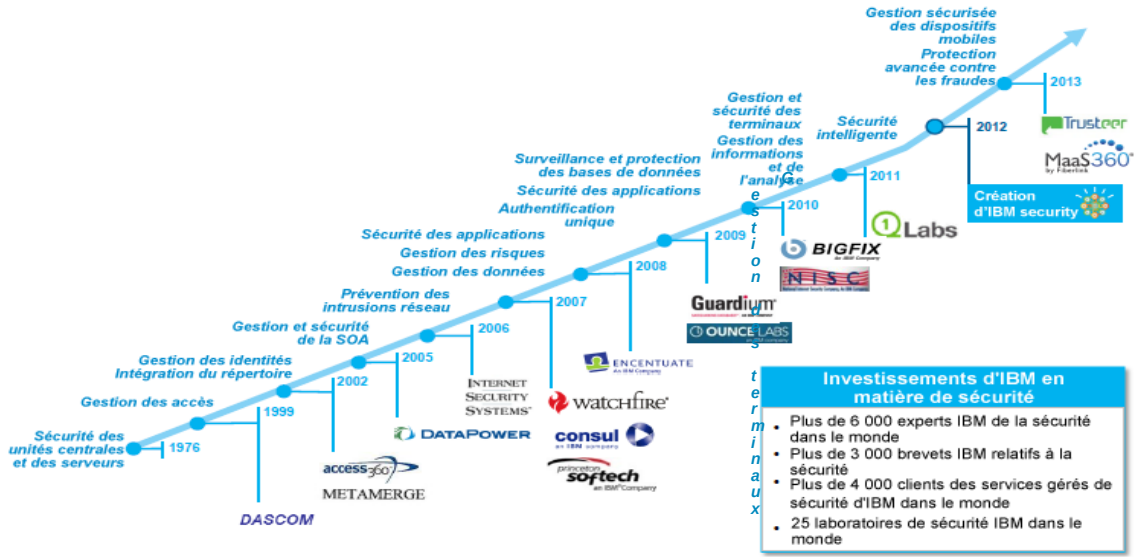
Il ne faut pas voir en la relative nouveauté du cloud et en ses défis uniques la possibilité d'apprendre « sur le tas » ; bien au contraire, il faut savoir se préparer dès le départ et faire montre d'une expertise exceptionnelle.

IBM est parfaitement équipé pour aider les organisations à adopter le cloud en toute sécurité. Comme d'aucuns le savent, la société est forte d'années d'expérience en matière de sécurité informatique. Avant même que le cloud ne s'impose comme le prochain tournant de l'informatique, IBM avait déjà développé sa solide infrastructure de sécurité. Conçus selon une approche pragmatique pour relever les défis de sécurité des centres de données privés complexes, nos éléments d'infrastructure sont extensibles aux environnements de cloud. En outre, la sécurité du cloud requérant une approche holistique plutôt que fragmentée, l'histoire d'IBM regorge d'exemples de croissance organique et d'acquisitions uniques en leur genre (voir la chronologie disponible à la page suivante) ayant contribué à la création d'un portefeuille complet de technologies de sécurité (logiciels et appliances virtuelles) et de services de sécurité professionnels et gérés.

Infrastructure de sécurité IBM

1

Chronologie de l'expansion du portefeuille de sécurité IBM

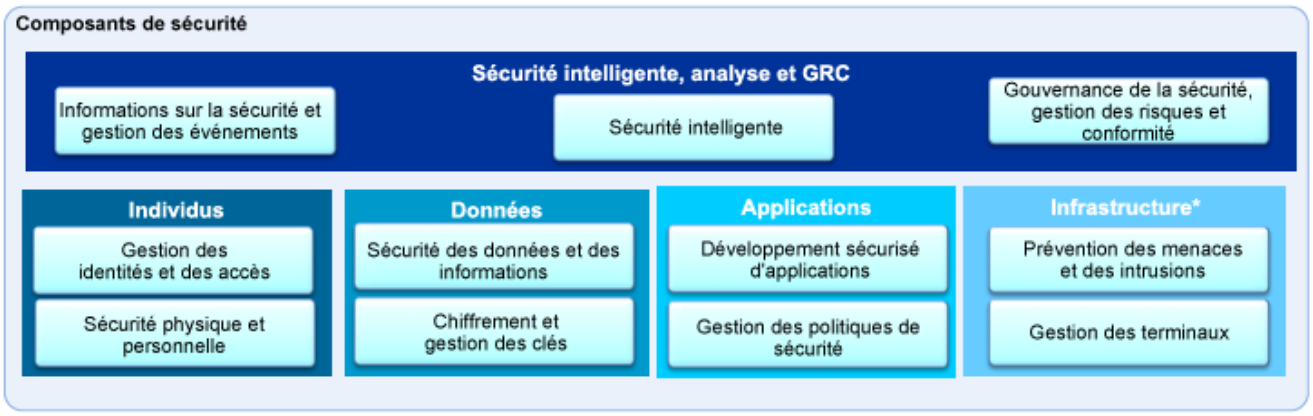


Source : IBM

Forte de son expérience acquise au fil des engagements clients, mais aussi grâce à ses leaders d'opinion internes ainsi qu'à l'un des plus grands bancs d'essai au monde (réalisé en interne), IBM a développé son architecture de référence pour le Cloud Computing (CCRA) pour favoriser l'adoption des services cloud. Naturellement, la sécurité est la base même de cette architecture.

De la CCRA aux engagements clients, IBM applique une approche stratégique s'appuyant sur des meilleures pratiques et reposant sur trois principes qui tirent parti des différents composants de son vaste portefeuille de sécurité :

1. Définir une stratégie de cloud en ayant la sécurité à l'esprit
2. Identifier les mesures de sécurité nécessaires
3. Mettre en œuvre la sécurité sur le cloud



Source : IBM

IBM, fournisseur de cloud sécurisé et de services de cloud privé

Comme nous l'avons déjà évoqué, le fournisseur de cloud et ses locataires se partagent les responsabilités en matière de sécurité. Et, l'ensemble de la sécurité n'étant que le reflet des éléments qui la composent, les couches de base de la sécurité et la protection des centres de données du fournisseur de cloud (responsabilité incombant au fournisseur) sont particulièrement cruciales. Comme prévu, les centres de données d'IBM conçus pour le cloud et ses pratiques en matière de sécurité du cloud adhèrent à son architecture CCRA.

Nous avons également expliqué que la mutualisation et l'accès Internet sont des éléments structurels des services de cloud public, et ces éléments augmentent les risques de sécurité. Même si des technologies et des pratiques de sécurité peuvent être mises en œuvre en vue d'atténuer ce risque supplémentaire, certaines réglementations (par exemple, la loi HIPAA (Health Insurance Portability and Accounting Act) relative à la santé et l'assurance maladie ou encore les normes PCI-DSS (Payment Card Industry Data Security Standards) relatives à la sécurité des données des applications de paiement) et directives relatives à la confidentialité des données (par exemple, la directive Safe Harbor (Sphère de sécurité) du ministère du Commerce des États-Unis) restent difficiles à appliquer. Effrayées par cette réalité, les organisations ont tendance à utiliser leurs centres de données sur site pour héberger les applications et charges de travail régies par ces réglementations et directives ; mais en appliquant cette stratégie, elles renoncent à l'évolutivité, l'agilité et aux avantages économiques (par exemple, aucun investissement de capitaux et facturation à l'utilisation) qu'offre le modèle de services cloud.

En 2013, l'acquisition de la société d'infrastructure de Cloud Computing SoftLayer a permis à IBM de combler l'écart qui existait entre les avantages du cloud et la sécurité des centres de données privés. Parfaitement ancrée dans l'automatisation du provisionnement et la gestion de serveurs physiques et virtuels et dans la gestion de la sécurité (par exemple, publication spéciale 800-53 du NIST (National Institute of Standards and Technology) et auto-évaluation STAR (Security, Trust and Assurance Registry) de la Cloud Security Alliance), IBM offre les services SoftLayer suivants :

- **Cloud bare metal SoftLayer** : combine le provisionnement à la demande de serveurs physiques dédiés aux clients hébergés dans les centres de données SoftLayer à la connectivité client via un port réseau privé.
- **Cloud privé SoftLayer** : combine le provisionnement à la demande de serveurs virtuels dédiés à un locataire unique hébergés dans les centres de données SoftLayer à la connectivité client via un port réseau privé.
- **Cloud public SoftLayer** : offre IaaS de cloud public hébergée dans les centres de données SoftLayer.

Lorsqu'ils sont combinés, ces trois services SoftLayer offrent aux clients IBM tous les services d'infrastructure de cloud sans aucune restriction quant à la prise en charge de leurs différentes charges de travail.

LE DERNIER MOT

Dans un monde axé sur une technologie en perpétuelle évolution, la sécurité requiert une approche adaptée passant par un investissement unique et un déploiement universel. Pour mettre en œuvre une telle approche, la sécurité doit faire l'objet d'une planification et d'une intégration, mais elle doit également s'adapter en fonction de la situation, et pouvoir être parfaitement contrôlée. Sans cette approche, la pratique de la sécurité dans les environnements de cloud demandera une grande réactivité et impliquera des opérations coûteuses et sous-optimisées.

- IBM dispose des atouts nécessaires pour optimiser la sécurité du cloud :
- IBM propose un portefeuille complet et éprouvé de technologies de sécurité extensibles aux environnements de cloud. IBM dispose de toutes les technologies mentionnées dans ce document. La société offre également des solutions de sécurité conçues pour relever les défis uniques inhérents à la sécurité des environnements de cloud (par exemple, l'atténuation des vulnérabilités de l'hyperviseur). En outre, son adhérence aux normes permet à IBM d'intégrer les actifs compatibles existants des clients.
- IBM applique une approche de l'adoption et de la sécurité du cloud ***stratégique*** (en permettant à l'entreprise d'évoluer grâce au cloud), ***holistique*** (un environnement de cloud est une instance dynamique d'un centre de données privé et doit de ce fait appliquer des meilleures pratiques de sécurité identiques) et ***proactive*** (en détectant et corrigeant les vulnérabilités précédant les menaces).

Et, comme pour un centre de données privé, les opérations de sécurité des environnements de cloud sont exécutées en permanence, 24 h/24 et 7 j/7. Les équipes dédiées à la fourniture de services de sécurité professionnels et gérés d'IBM mettent au service des organisations leur expertise et les pratiques fiables et éprouvées dont elles ont besoin.

Michael Suby

Vice-président de la recherche
Stratecast | Frost & Sullivan
msuby@stratecast.com

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041,
États-Unis
Tél : +1 650 475 4500
Fax : +1 650 475 1570

San Antonio
7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616,
États-Unis
Tél : +1 210 348 1000
Fax : +1 210 348 1003

Londres
4, Grosvenor Gardens,
London SWIW ODH, RU
Tél : +4420 7730 3438
Fax : +4420 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

À PROPOS DE STRATECAST

Stratecast collabore avec ses clients pour les aider à prendre des décisions de gestion intelligentes sur les marchés hyperconcurrentiels et en évolution rapide des technologies de l'information et de la communication. Sous la forme d'une combinaison de rapports d'études à vocation pratique disponibles par abonnement et de prestations de conseil personnalisées, Stratecast fournit des informations et des perspectives d'ensemble que seules permettent d'obtenir des années d'expériences concrètes dans un secteur où les clients sont aussi des collaborateurs, les partenaires d'aujourd'hui sont les concurrents de demain, et où l'agilité et l'innovation sont des ingrédients indispensables de la réussite. Prenez contact avec votre responsable de compte Stratecast afin de mobiliser notre expérience pour vous aider à atteindre vos objectifs de croissance.

À PROPOS DE FROST & SULLIVAN

Frost & Sullivan, la Société du Partenariat de Croissance, travaille en collaboration avec ses clients pour tirer parti d'innovations visionnaires qui répondent aux défis mondiaux et aux opportunités de croissance associées qui feront ou briseront les acteurs actuels du marché. Depuis plus de 50 ans, nous avons développé des stratégies de croissance pour les 1 000 plus grandes entreprises internationales, les sociétés émergentes, le secteur public et la communauté des investisseurs. Votre organisation est-elle prête pour le prochain déferlement de convergence sectorielle, de technologies révolutionnaires, d'intensification de la concurrence, d'hypertendances, de meilleures pratiques innovantes, de dynamiques clients changeantes et d'économies émergentes ? Nous contacter : Commencer la discussion