Enjeu : le Cloud au service des métiers

D'après de nombreux sondages, la sécurité apparaît comme le principal frein à l'adoption du Cloud dans les organisations.

Malgré des réserves justifiées sur les questions de confidentialité, de contrôle et de lieu de stockage des données, le Cloud poursuit son irrésistible ascension depuis une décennie. Une étude Gigaom[1] a d'ailleurs récemment confirmé cette « volonté d'avancer au mépris du danger ». Sur les 500 décideurs informatiques interrogés, 71 % utilisent désormais des solutions SaaS (Software as a Service), ce malgré quelques interrogations sur la sécurité. Pourquoi ? C'est très clair : ces solutions sont à la fois plus économiques et plus agiles que les alternatives « maison ».

Autre hypothèse : nous avons peut-être atteint un stade où les pressions commerciales sont telles que les avantages des services Cloud sont devenus incontournables. À moins que nous n'assistions à une évolution plus positive, vers davantage de confiance dans l'informatique dans le nuage ?

Le Cloud en soi n'a rien de nouveau. L'idée d'un accès externe à une informatique centralisée via un réseau mondial existe en effet depuis les années 1960. Depuis, pour dissiper les inquiétudes sur les questions de confiance et de sécurité, les géants du Cloud hybride et public ont massivement investi dans leurs infrastructures de sécurité – une stratégie qui semble aujourd'hui porter ses fruits.

Lorsqu'aux États-Unis, la très prudente communauté du renseignement fait appel à un acteur du Cloud pour fournir à la CIA et la NSA des services informatiques et analytiques facturés à l'usage, c'est bien que le vent est en train de tourner. Dans une allocution publique en 2014, Douglas Wolfe, le Directeur des systèmes d'information de la CIA, a qualifié la décision d'investir 600 millions de dollars dans un Cloud développé par Amazon Web Services « d'investissement technologique le plus important de ces dernières années », avec des implications qui dépassent de loin le cadre technologique. Assiste-t-on à la mort des data centers physiques dans l'entreprise ? C'est peu probable, car malgré ce soutien public en faveur du Cloud, le service fonctionnera derrière le pare-feu des agences de renseignement concernées. Dans les faits, il s'agira donc d'un Cloud public sur un site privé.

Nous prévoyons une généralisation de l'usage de technologies comme VMware, KVM et OpenStack dans les entreprises qui souhaitent virtualiser leur environnement pour bénéficier des avantages d'un Cloud privé, tant en termes de coûts que de gains d'efficacité opérationnelle.

Dans cette optique, NTT Security a établi des partenariats avec plusieurs entreprises dans le monde pour mettre en place un accès réseau sécurisé, collaboratif et pratique à un pool mutualisé de ressources informatiques (serveurs, infrastructures de stockage, applications et services). Dans ce document, nous présentons les stratégies, processus et technologies appelés à transformer votre data center. Vous passerez ainsi d'une structure statique, où les applications tournent sur des serveurs dédiés, à un environnement dynamique, flexible et automatisé. L'objectif : permettre à vos utilisateurs d'accéder aux ressources informatiques et applications dont ils ont besoin, en tout lieu, à tout moment et depuis n'importe quel terminal. Quel que soit le modèle de Cloud envisagé – privé, public ou hybride – nous vous accompagnons à travers toutes les étapes de la création d'une architecture de sécurité capable de vous protéger, de monter en capacité et d'évoluer au rythme de vos impératifs métiers et réglementaires.

1. Gigaom, enquête auprès d'acheteurs informatiques et de services cloud stratégiques, 2014

1. Le Cloud comme outil de rapprochement avec les métiers

Lorsqu'ils nous demandent notre avis d'expert sur les contrôles de sécurité dans le Cloud, nos clients apprennent avec un certain soulagement que nous déconseillons de traiter à part ce volet infrastructurel. Les entreprises ont investi massivement dans des politiques et des frameworks de gouvernance ad hoc, y compris pour les environnements virtuels. De fait, elles fuient comme la peste toute complexité supplémentaire. La bonne nouvelle, c'est qu'une migration vers le Cloud n'impose pas systématiquement la création d'une architecture de sécurité entièrement nouvelle.

Le Cloud appelle cependant à une approche différente de la sécurité. Pourquoi ? Jusqu'ici, applications et données stratégiques étaient généralement conservées séparément sur des réseaux physiques, leur accès étant contrôlé par des règles définies sur des pare-feu et des systèmes de gestion des accès et des identités (IdAM). Or, la virtualisation et le Cloud étant basées sur la mutualisation des ressources, difficile d'appliquer des principes de zero trust (zéro confiance) avec les technologies existantes. Ajoutez encore à cela des utilisateurs exigeant d'accéder immédiatement aux applications virtuelles et Cloud, alors qu'en environnement physique, il fallait généralement attendre plusieurs jours en raison de procédures et de tests rigoureux. C'est donc aux professionnels de l'informatique et de la sécurité de l'information que revient la responsabilité de trouver un juste équilibre entre attentes et risques, au vu des éléments dont ils disposent sur les menaces présentes et futures.

En soi, le Cloud ne génère pas plus de risques, mais l'environnement ouvert de la virtualisation favorise le détournement d'applications courantes pour contourner les contrôles en place. Avec la centralisation des données et certains compromis sur la sécurité au nom de la performance et de l'efficacité, les attaques sont plus difficiles à détecter et à enrayer.

2. Des critères de décision basés sur les risques pour toutes les applicationss

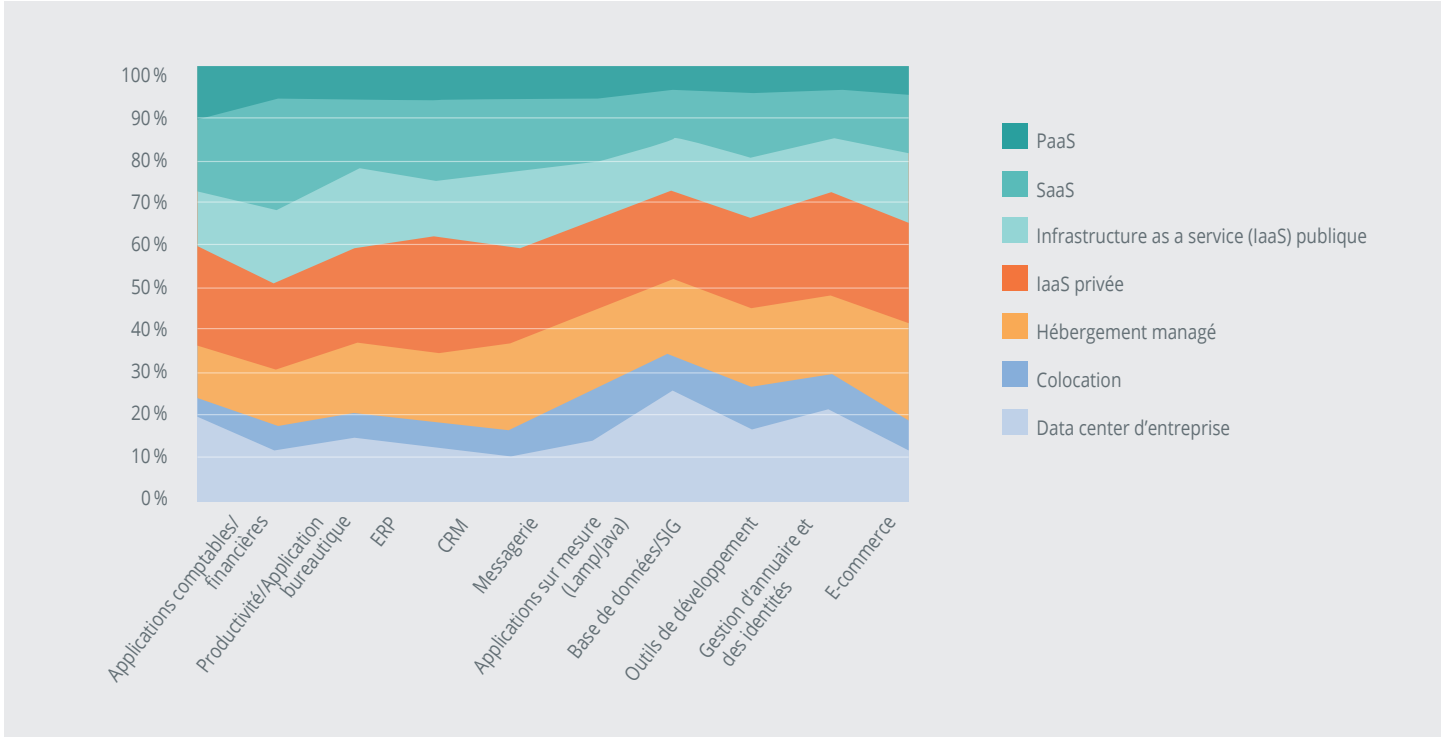
La sécurité dans le Cloud commence par un référencement exhaustif de tous les services et applications dans un listing de fournisseurs agréés, dont l'accréditation sera notamment octroyée en fonction des risques qu'ils représentent.

Dans son rapport Cloud Reality Check 2015, NTT Communications[2], synthétise les conclusions d'une enquête réalisée auprès d'environ 1 600 décideurs dans le domaine des TIC en France, en Allemagne, au Benelux, en Espagne, au Royaume-Uni et aux États-Unis. D'après ce rapport, près de 10 % des applications ont vocation à ne jamais migrer vers le Cloud, notamment dans les secteurs industriels et les branches ultra réglementées. Mais au-delà de cet état de fait, le rapport pointe les incohérences du modèle de déploiement applicatif des entreprises.

Les personnes interrogées affichent cependant clairement leur ouverture au déploiement ou à la migration de leurs applications métiers critiques (progiciels de gestion intégrée (ERP), systèmes de gestion de la relation client (CRM) et plateformes e-commerce) vers une infrastructure Cloud, avec différents niveaux de contrôle et de personnalisation. C'est généralement à ce stade que nous entrons en jeu pour aider nos clients à établir, en concertation avec les métiers, le bon équilibre entre Cloud privé et Cloud public. Nous les accompagnons également dans leur analyse des flux de données et, surtout, de leurs avantages en termes de productivité, de collaboration et de performance.

Si nous plaçons ces discussions sur un plan « business », nous y apportons également des compétences technologiques approfondies. Nous validons l'identité des applications de votre data center pour être certains qu'elles n'utilisent que les ports standards. En procédant ainsi, nous barrons la route aux applications malveillantes et appliquons des mesures de prévention des infections par malware de votre entreprise.

Figure 1 NTT Communications, Cloud Reality Check 2015 : D'après vous, quel est le modèle de déploiement le mieux adapté à chacune des applications suivantes ? (Tous pays)



2. NTT Communications, Cloud Reality Check 2015

3. Prioriser la mise en œuvre des contrôles

Une fois les critères de risques établis, la DSI peut travailler au contact des métiers pour prioriser les contrôles à appliquer de manière cohérente à l'ensemble des services Cloud, à commencer par les politiques de prévention des pertes de données, le cryptage de données, la gestion des accès et des identités, et le contrôle des modifications.

Cette démarche permet d'harmoniser les politiques sur site et dans le Cloud, avec à la clé des vérifications et des contrôles plus homogènes. Le Cloud n'est pas condamné à rester un sujet de discorde entre IT et métiers. En fait, nous avons constaté sur le terrain que le Cloud permettait de rapprocher les métiers et la DSI dès lors que celle-ci impulse l'adoption du Cloud dans une démarche de productivité et de rationalisation des coûts, tout en fiabilisant les dispositifs de sécurité de l'entreprise par une plus grande automatisation des contrôles et une accélération des déploiements.

4. Des politiques plus rapidement applicables pour adapter le Cloud au rythme de l'activité

Le terme de pare-feu rassure ; il évoque un système de défense solide et inviolable. Dans un environnement Cloud ou virtuel, les entreprises recherchent des solutions apportant le même niveau de protection et de contrôle zero trust, avec en prime des performances et une flexibilité revues à la hausse.

Au fil du temps, bon nombre d'entreprises ont érigé un véritable rideau de pare-feu imposant des centaines de règles à l'origine de processus complexes et gérés par de multiples outils. Si l'arrivée de la virtualisation et du Cloud n'aggrave pas forcément le problème, il n'en reste pas moins que les organisations font trop souvent l'impasse sur l'étude ou l'examen des possibilités qu'offre le Cloud. Il en résulte une version virtuelle d'une appliance de sécurité, avec ses ports et ses protocoles, qui ne fait qu'ajouter aux problèmes de gestion. Pour éviter cet écueil, une nouvelle approche de la mutualisation des ressources informatiques permettra de faire un bilan des parcs de pare-feu existants et de les optimiser. Chez NTT Security, nous collaborons avec des entreprises à l'élaboration de contrôles simples et cohérents pour les pare-feu de nouvelle génération et les systèmes de protection contre les menaces avancées.

Nous utilisons pour cela des outils de gestion natifs qui concrétisent les avantages des environnements virtuels et Cloud en termes de vitesse et de coûts.

5. Vers une politique du zero trust dans le Cloud

Beaucoup d'entreprises avec lesquelles nous discutons ont à cœur de répliquer les principes du zero trust dans les environnements virtuels et Cloud. Leurs objectifs sont multiples :

1. Contrôler les accès selon les applications, les niveaux de charge ou l'identité des utilisateurs
2. Bloquer les applications potentiellement malveillantes ou mal configurées
3. Empêcher les menaces connues et inconnues de compromettre le réseau et d'évoluer latéralement
4. Mettre en œuvre des règles de prévention des menaces spécifiques aux applications

Les entreprises sont impatientes d'atteindre ces objectifs pour déployer leurs applications en fonction des utilisateurs, des applications elles-mêmes et des contenus, sans concession sur la performance. Forts de notre expérience dans ce domaine, nous accompagnons les entreprises vers ces objectifs.

Conclusion : nous mettons le Cloud au service de votre entreprise

Le Cloud Computing est là pour durer. Selon le rapport Cloud Reality Check, les entreprises prévoient une hausse de leur budget cloud de 6 % actuellement à 28 % d'ici 2018[3]. Face à des entreprises soucieuses d'exploiter tous les avantages du Cloud, notre mission est de les accompagner vers cet objectif, tout en maîtrisant les risques, la complexité et les coûts. De nombreuses entreprises ont déjà franchi le pas, par le biais de projets de virtualisation ciblés ou du déploiement d'applications en mode SaaS. Mais sans planification adéquate ni approche stratégique et coordonnée du Cloud, bon nombre de ces projets ne pourront générer le retour sur investissement ou les économies d'échelle espérés.

C'est pourquoi nous aidons nos clients à prendre le contrôle de leurs projets Cloud, dans une démarche de collaboration avec les métiers pour définir le cahier des charges et les objectifs. Si la DSI n'assure pas la maîtrise des projets Cloud, les changements se feront, certes, mais de façon fragmentée. Or, l'expérience nous a prouvé qu'outre l'impact négatif sur l'activité, l'apparition d'une « informatique parallèle » est source de risques pour l'entreprise. Enfin, au moment d'établir leur plan d'évolution vers le Cloud, les entreprises devront définir les points charnières qui marqueront un passage vers chaque nouvelle étape. Ainsi, certains déclencheurs technologiques comme les cycles de renouvellement d'équipements, les grands projets applicatifs et les fusions et acquisitions offrent autant d'occasions d'aller de l'avant, tout en protégeant les investissements existants et en rentabilisant le projet global.

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.

3. NTT Communications, Cloud Reality Check 2015