SPÉCIAL COVID-19

Après avoir fait preuve d'une réticence parfois justifiée – nous verrons pourquoi – de plus en plus d'entreprises se laissent séduire par le cloud, son caractère hyperfonctionnel et économique. *«Tout d'abord parce que, hormis leur activité liée à leur cœur de métier, les entreprises génèrent de plus en plus de données, de tout genre, qu'il est nécessaires de stocker,* explique Yves Pellemans, directeur technique d'Axians (certifié Iso 27000 et Anssi). *Or, même si le stockage en tant que tel coûte bien moins cher qu'il y a quelques années, nos clients cherchent avant tout des outils pour stocker facilement leurs données et mettre à jour leurs logiciels et leurs systèmes d'exploitation.»* Ainsi, en plus des ses fonctions de sauvegarde, de mise en réseau et d'analyse de données, de mégadonnées ou de big data, d'accès à des applications bureautiques standards ou d'exécution de systèmes opérationnels plus complexes, s'ajoutent aujourd'hui la possibilité de gérer, grâce au cloud, les interactions entre les objets connectés grâce aux progrès de l'intelligence artificielle et une meilleure communication machine to machine (M2M). De nombreuses raisons donc de s'intéresser au cloud…

© Getty Images

Un réel engouement donc

Selon une récente enquête, environ 70 % des entreprises utiliseraient le cloud (public, privée, mixte). D'ailleurs, à en croire le cabinet 451 Research, *«cette dépendance croissante envers des sources externes de services d'infrastructure, d'applications, de gestion et de sécurité a pour effet de diminuer les dépenses dans l'informatique traditionnel au profit d'investissements massifs dans cette technologie (hébergement et achats de services et de matériels confondus)»*.

Pourquoi ce net regain d'intérêt ? La digitalisation des entreprises n'y est pas pour rien. S'y ajoutent, nous l'avons déjà souligné, la rationalisation des coûts en matière d'IT. Et la sécurité. Longtemps considérée comme un frein, la sécurité des données est désormais perçue comme un atout du cloud. La preuve : le cloud est de plus en plus utilisé par la banque et l'assurance. *«Aujourd'hui, les entreprises veulent non seulement stocker leurs données de manière sécurisée mais aussi trouver des solutions pour que ces données soient toujours disponibles. On n'a pu le constater pendant le confinement : sans le cloud, de nombreuses entreprises auraient été incapables de basculées en quelques jours, voire quelques heures, en mode "télétravail"»*, explique Yann Fralo, Country Manager France chez A10 Network.

Stéphane de Saint Albin, président de Rohde & Schwarz Cybersecurity France et vice-président d'Hexatrust, ajoute : *«La sécurité du cloud ne constitue plus le frein à son utilisation comme elle pouvait encore l'être il y a quelques années. Aujourd'hui, on trouve sur le marché des solutions qui permettent de stocker et de gérer sur le cloud ses données, sans pour autant renoncer à y appliquer des mesures de sécurité strictes, et sa souveraineté sur ses propres données.»*

UNE LISTE DE PRESTATAIRES DE L'ANSSI

L'Anssi met à votre disposition sur son site une liste des prestataires d'informatique en nuage qualifiés.
→ **www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/**

DU CÔTÉ DES FABRICANTS

STEVEN COMMANDER

Directeur de la prescription chez HID Global

© DR

«LE CLOUD FAIT PARTIE DU QUOTIDIEN DE NOS MÉTIERS.»

«Le cloud fait aujourd'hui partie du quotidien de nos métiers. Et il sera de plus en plus utilisé. Ne serait-ce qu'avec le recours de plus en plus important au badge dématérialisé sur un smartphone, par exemple. Les technologies du contrôle d'accès seront intégrées dans le smartphone ou directement dans les applications de l'entreprise grâce aux technologies dans le cloud comme le SDK ou l'API… Mais tout cela ne pourra se faire que si nous parvenons à rassurer nos clients. Non seulement en respectant certains règlements comme le RGDP, mais en nous appuyant aussi sur les bonnes pratiques.»

© Getty Images

La souveraineté : un vrai problème

Stéphane de Saint Albin pointe un vrai problème du cloud : la souveraineté des données. *« On peut accepter le cloud sans pour autant abonner toute forme de souveraineté sur ses données et leur valeur stratégique,* poursuit donc le vice-président d'Hexatrust. *Mais il ne faut pas faire preuve de naïveté. Car les données qui sont stockées dans un cloud américain, par exemple, peuvent susciter l'intérêt… Il faut donc être très vigilant en matière de chiffrement, faire en sorte qu'il soit unique et en possession de personne d'autre que soi. »*

Or, rester souverain est possible. *« Les données stockées sur le cloud peuvent être excessivement sensibles, critiques… Structurées on non,* explique Luc d'Urso, président directeur général d'Atempo. *Nous devons absolument protéger ce patrimoine. L'alternative aux acteurs américains existe ; nous disposons d'hébergeurs et d'éditeurs souverains de grande qualité et ils ne sont pas assujettis au Patriot Act ! Nous devons également nous protéger des lois d'extraterritorialité du droit américain. Nous avons perdu la guerre du hardware, mais nous disposons de tous les atouts pour remporter celles de l'hébergement et du traitement des données*

3 QUESTIONS À

DENIS BRUNEL

Directeur sûreté de Capgemini

© DR

Il semble qu'à l'occasion de la crise du Covid-19 et de la mise en place du confinement, certaines entreprises découvrent l'intérêt du cloud. Est-ce votre cas ?

Le cloud est depuis longtemps un des outils dont Capgemini se sert dans le cadre de son activité. Et grâce à sa maîtrise, nous avons pu, dès l'annonce par le président de la République de l'entrée en vigueur du confinement, le 17 mars, mettre, très vite et avec beaucoup d'agilité, 99 % des 25000 collaborateurs travaillant sur les 64 sites du groupe en télétravail… Tout en gérant de manière centralisée nos solutions de contrôle d'accès, de vidéosurveillance, de lutte contre l'intrusion, notre télésurveillance, notre sécurité humaine… Si nous en sommes là, c'est que dès 2019, j'ai entamé une migration majeure de notre système de contrôle d'accès désormais déployé, aussi, dans Security Command Center (CCC).

Quel élément vous a incité à franchir le pas du cloud alors que certains de vos confrères font toujours preuve d'une certaine méfiance à son égard ?

Le cloud me permet de mieux gérer les procédures et de manière centralisée. Il me permet ainsi d'avoir un niveau de qualité homogène en matière de techniques, de respect des procédures, de résilience… Nous pouvons aussi, le cas échéant, basculer en mode supervision réseau pour voir l'état de notre système. Par contre, je ne suis pas prêt à tout virtualiser, à tout mettre sur le cloud. Car s'il est assez simple de sécuriser l'accès physique aux datacenters, d'assurer la sécurité des bâtiments grâce à de la vidéo-surveillance, du contrôle d'accès, de l'anti-intrusion…, il faut garder à l'esprit qu'en matière de sécurité le maillon le plus faible est souvent l'humain. Il faut donc prévoir des procédures de sécurité, de contrôle… qui permettent de sécuriser les données du serveur jusqu'au poste de l'opérateur et de détecter toute menace éventuelle, tout comportement déviant…

Quel bilan tirez-vous du recours au cloud pendant le confinement et comment envisagez-vous la reprise de l'activité au sein de Capgemini ?

Cette période aura évidemment fait apparaître des points d'amélioration. Et le bien-fondé de certaines approches comme la Track Force, une solution dématérialisée de suivi des incidents avec report des informations vers le responsable de site et le responsable sécurité. Nous avons aussi pu, grâce au cloud, gérer de manière très souple le paramétrage de systèmes de sécurité comme celui des alarmes, par exemple. Enfin, je pense que le cloud nous permettra de sortir de la crise aussi facilement que nous y sommes entrés et de reprendre, avec beaucoup de souplesse, notre activité.

professionnelles et de leur sécurité grâce à des software français, souverains.»

■ *Quelles données sur le cloud ?*

«Toute entreprise génère de la donnée. Dans une usine, une machine, un testeur, un détecteur… produisent de la donnée. Ces dernières peuvent être mises à disposition des managers, des équipes techniques, des opérateurs… pour savoir comment a été produit tel ou tel bien, quel incident a pu survenir lors de la phase de production…, explique Laurent Laporte, président directeur général de Braincube. *Il y a donc deux manières d'utiliser ces données : de manière continue afin d'aider à mieux piloter l'usine, ou en les stockant pour faire du big data, du machine-learning… L'intérêt du cloud est de permettre de stocker des données qui pourront être brassées et utilisées pour améliorer les process de l'entreprise. Pour* ● ● ●

PAROLE D'EXPERT

CHRISTOPHE ROSSI
Président directeur général de CNCR Group


© DR

«CONTRÔLER LE RESPECT DES PROCÉDURES DE SÉCURITÉ.»

«Le cloud modifie profondément les modes de production de l'IT. Il requiert un outil management de la End-User Experience. Pour comprendre les usages, dimensionner le service et maîtriser le niveau de performance délivré. Pour contrôler la sécurité et la conformité des Workplaces. C'est ce que nous proposons avec Interact. L'expérience de l'utilisateur est quantifiée et détaillée pour chaque application, chaque site, chaque type de configuration... de bout en bout.
Pour la sécurité, certaines données sont focalisées sur le niveau de vulnérabilité du SI depuis les postes de travail : conformité logicielle, état de fonctionnement des dispositifs de protection, comportement à risque des utilisateurs, shadow IT, etc. Interact s'intègre dans l'écosystème en alimentant les outils dédiés à la sécurité du SI comme les SIEM (Security information and Event Management) et les SOC (Security Operation Center). Interact permet par exemple de détecter si l'antivirus est à jour, si le pare-feu est activé, si un PC a une session non verrouillée sans utilisateur actif, si un compte administrateur local du poste est non désactivé, si l'utilisateur a un comportement "à risques"… Tout cela, évidemment, dans le cadre du respect de la réglementation RGPD.»

© Getty Images

● ● ● *leur assurer la sécurité de leurs données, nos deux datacenters sont installés en France, à Lyon et à Paris, et nous sommes certifiés ISO 27000 et nous plions aux recommandations de l'Anssi.»* Peut-on tout confier au cloud ? Pour Stéphane de Saint Albin, *«il faut évidemment se poser la question des données qu'on souhaite stocker dans le cloud. Certaines sont plus critiques que d'autres et peuvent revêtir un caractère vital pour l'entreprise».*

«Le volume de données va croître au rythme de 60 % annuel sur les cinq prochaines années. Il s'agit d'un gisement énorme qu'il faut absolument sécuriser car il constitue une source extraordinaire de création de valeur pour l'Europe. Nous devons également proposer des solutions souveraines pour corréler ces données pour en tirer la quintessence, insiste Luc d'Urso. *Le cloud hybride va donc naturellement s'imposer en distinguant les données chaudes qu'on utilise au quotidien, qui resteront stockées sur site, au plus proche de la puissance de calcul, et les données froides à archiver ou à utiliser ponctuellement. Il faut arbitrer entre les données critiques, vitales, et celles qui le sont moins…»*

■ *Et la sécurité dans tout ça ?*

La sécurité ne serait donc plus un frein à l'utilisation du cloud ? *«Nous nous heurtons moins à des refus définitifs. Et lorsqu'on prend le temps d'expliquer les choses, de faire de la pédagogie, les directeurs sûreté, les DSI… comprennent que ce n'est pas parce qu'on est dans le cloud que tout est moins sécurisé,* insiste David Brillant, Director Sales Engineering South EMEA chez Forcepoint. *Par exemple, Forcepoint a reçu le "visa sécurité de l'Anssi". Par ailleurs, je pense qu'il y aura un avant et un après Covid-19. À cette occasion, les DSI se sont rendus compte que le cloud facilitait grandement la continuité de l'activité de l'entreprise. Ne serait-ce que pour le télétravail. Sans nuire à sa sécurité de l'entreprise.»*

Il ne faut pas se laisser aveugler par le caractère «nuageux» du cloud. Cela reste du stockage comme un autre. Physique et quelque part. *«Avant d'entrer dans le débat sur le stockage en local ou pas, rappelons qu'il ne faut plus raisonner en termes de sécurité physique. Elle est importante certes mais ce n'est plus, selon moi, le cœur du débat, explique Cédric Cailleaux, responsable technique cybersécurité & RSSI chez Axians. En effet, il est désormais possible de connaître la qualité et la fiabilité des capacités d'hébergement d'un datacenter. Facilement reconnaissable au travers de leur qualification en quatre niveaux : allant de tiers 1 à tiers 4. Ce dernier étant le niveau le plus élevé puisqu'il assure que les données ne seront pas indisponibles plus de 20 minutes par an. Le tiers 4 est assez rare mais pour la majorité des besoins exprimés par les entreprises, on peut tout à fait se satisfaire d'un datacenter tiers 3+, par exemple.»*

Yann Fralo ajoute : *«Il n'y a aucune raison de faire moins en matière de sécurité sur le cloud que ce qu'on fait localement, sur ses propres réseaux et moyens de stockage. On peut tout à fait demander à son fournisseurs cloud de respecter un cahier des charges précis, ne pas hésiter à l'auditer pour s'assurer des standards sécurité qu'il applique.»* Point de vue que partage Philippe Rondel, Senior Security Architect chez Check Point Software : *«Il nous faut accompagner les utilisateurs dans la création de leur environnement et outil cloud. Les aider à sécuriser leurs réseaux et à analyser leur environnement, les informations et l'accès à l'ensemble. Checkpoint nous faisons en sorte de leur fournir les outils qui leur*

PAROLE D'EXPERT

GABRIEL GEDDA

Président du chapitre France d'Asis International et EMEA Sub-Regional Physical Security Manager France-Benelux chez AP Global Physical Security


© DR

«LE CLOUD PARTICIPE À LA CONTINUITÉ DE L'ACTIVITÉ.»

«Le Covid-19 et le confinement vont aider certains directeurs sûreté et DSI à prendre conscience de l'intérêt du cloud en cas de crise. Ne serait-ce que pour permettre la continuité de l'activité via le télétravail, par exemple. Le cloud est un disque dur externe à l'entreprise dont l'un des buts, grâce à la digitalisation, est de basculer, en cas de crise, dans un mode de fonctionnement qui lui permettra de maintenir son activité dans les meilleures conditions. Le cloud permet au directeur sûreté de gérer à distance, et de fermer par exemple, les différentes sites de son entreprise, en supprimant, de manière très souple, simple, rapide, les droits d'accès aux divers sites ou en limitant le nombre aux équipes nécessaires au bon fonctionnement de l'activité tout en ayant une vue holistique de son activité grâce au Dashboard dynamique.»

SPÉCIAL COVID-19

DU CÔTÉ DES FABRICANTS

VINCENT DUPART

Président directeur général de STid

© DR

« LE CLOUD EST UNE VRAIE TENDANCE DANS LE CONTRÔLE D'ACCÈS. »

« Le cloud est très utile dans les métiers de la sécurité électronique et est devenu une vraie tendance dans le monde du contrôle d'accès. Il permet de gérer de manière dynamique les droits. Le gestionnaire des droits peut ainsi accéder, de partout dans le monde, à une plateforme qui lui permet de gérer et d'accorder des droits à des utilisateurs, à des visiteurs. Chez STid, nous proposons des accès sécurisés par mots de passe forts, un hébergement sécurisé certifié pour les industries les plus exigeantes et un système de confidentialité de bout en bout conforme Cnil et RGPD pour protéger les données sensibles. S'y ajoute du chiffrement des BDD SQL avec possibilité de délégation d'administration sans accès au contenu/dissociation des droits d'accès et journalisation avec gestion des historiques.
En ce qui concerne le stockage physique des données, nous proposons une redondance totale avec deux datacenters.
Et pour les politiques de sécurité les plus exigeantes, nous proposons des solutions 100 % offline avec l'outil SECard qui permet de programmer vos badges et smartphone en local. »

permettent de "surveiller" leurs réseaux, leur cloud… afin de vérifier que leur fonctionnement et leur utilisation sont conformes aux règles de sécurité de l'entreprise et d'identifier, très vite, en temps réel, les failles sécurité ou les possibles actes malveillants. »

■ *Être exigeant et vigilant*

Le cloud a souvent suscité une certaine forme de psychose. Et pas toujours à tort. Tout le monde se rappelle du Patriot Act de 2001, du Privacy Shield de 2016 et plus près de nous du RGPD ou du cloud Act… Les Américains se sont dotés de moyens de contrôles des données. Et l'extraterritorialité du droit nord-américain peut être un danger lorsque des données sont stockées dans les cloud de Microsoft, Amazon et Apple… *« Il existe une vraie problématique sur la confidentialité des données* ● ● ●

2 QUESTIONS À

STÉPHANE LEMÉE

RSSI et directeur de la sûreté chez Fujitsu France

© DR

Quel est l'intérêt du cloud dans le cadre de vos fonctions ? Pourquoi l'utilisez-vous ?

Les solutions de sûreté telles que la vidéoprotection ou le contrôle d'accès sont désormais proposées dans le cloud et offrent de déporter l'infrastructure de traitement et de stockage des données pour ne conserver sur site que les caméras, lecteurs de badges et autres dispositifs contribuant à la sécurité des installations. Au-delà du gain financier et d'offrir l'agilité recherchée lors de déploiements (nouveau site, changement de technologie), le recours au cloud permet de simplifier la continuité de l'activité de l'entreprise et surtout sa reprise après sinistre. L'adoption du cloud permet enfin d'adresser les nouveaux usages comme le travail à distance, voire aux domiciles des intervenants, avec le recours massif au télétravail, y compris pour des profils jusqu'à présent exclus de ces solutions de repli.

Quels sont les freins au recours au cloud ?

En assurer la sécurité est, sans surprise, l'un des plus grands défis à relever pour l'adoption du cloud en France pour des raisons évidentes liées à la conformité (RGPD) et à la confidentialité de données du patrimoine informationnel de l'entreprise. Ce défi est amplifié par la carence en compétences constatée par près de deux tiers des entreprises au sein des équipes internes (DSI) qu'il faut alors compenser par un accompagnement externe. Si l'adoption du cloud permet de contribuer très fortement à sécuriser des installations de sûreté en permettant, par exemple, un déploiement très régulier des correctifs de sécurité, il convient de s'assurer d'une visibilité sur les informations échangées (DLP, CASB), de renforcer la gestion des identités comme du poste de travail, et d'adapter nos capacités de prévention et de détection (veille, SOC).

● ● ● *liées aux cloud public américains,* tient à souligner Cédric Cailleaux. *Il faudra donc être vigilant. En outre, il existe de nombreux moyens de s'assurer de la bonne gouvernance, du sérieux des hébergeurs, fournisseurs… : la famille ISO 27000, l'ISO 20000 et ISO 27701…, le respect des règles de l'Anssi et sa liste "SecNumCloud", les préconisations de la Cloud Security Alliance ainsi que l'agrément HDS qui concerne l'hébergement des données de santé… Ensuite, il faut inventorier ses actifs et savoir précisément où se situe la valeur de l'entreprise… »*

Une fois cela fait, vous pourrez définir des mesures de sécurité physique et logique pour protéger vos données, en transit ou en repos, contrôler les accès à votre réseau et gérer les identités. Puis prendre des mesures opérationnelles vous permettant de surveiller l'utilisation des données, par qui, comment…

■ *Lutter contre la malveillance*

Une fois vos données sur le cloud, vous pouvez vous doter des moyens de les surveiller, ainsi que le fonctionnement de votre réseau. *« Il existe des outils qui permettent d'analyser le contenu de toutes les données de l'entreprise, stockées sur le cloud ou en transit, afin de détecter tout comportement déviant, tout acte de malveillance,* explique David Brillant. *On pourra surveiller ce que fait l'utilisateur, ce qu'il télécharge, les documents qu'il consulte, les comportements inhabituels, les matériels qu'on connecte sur le réseau et s'ils sont autorisés ou fournis par l'entreprise, si certains consultent, sans en avoir le droit, des données confidentielles… »*

Cela permettra de signaler très vite au directeur sûreté et au DSI, les comportements suspects, les possibles menaces… afin qu'ils puissent prendre les mesures nécessaires pour préserver le patrimoine matériel et immatériel de leur entreprise. ■

SUR LE TERRAIN

JÉRÔME COMIN

Expert de Resadia du groupe Scopelec usages et services

© DR

« ÊTRE TRÈS EXIGEANT EN MATIÈRE DE SÉCURITÉ. »

« Resadia est un réseau regroupant 29 PME locales spécialisées dans l'intégration de services pour l'infogérance IT, les solutions Lan, la sécurité et la sûreté. Les entreprises s'intéressent de plus en plus aux potentialités du cloud en matière de sécurité. Mais il nous faut faire encore preuve de pédagogie. Le cloud a en effet des avantages. Il permet par exemple de mutualiser les expertises et de réduire les coûts. Mais il faut se poser la question des données qu'on y stocke et sur quel type de cloud : public, privé, mixte… À mon sens, le cloud public proposé par les Gafam pose des problèmes en matière d'extraterritorialité. Par ailleurs, les datacenters ne sont pas toujours en France… Il faut donc être très vigilant quant au choix de son prestataire et de ce qu'on attend de lui en matière de sécurité physique et logique. »