softwareONE

Gold
Business
Partner

IBM

CLOUD 3.0 : ÉTAT DES LIEUX ET MODES DE PROTECTION

Bienvenue dans la nouvelle ère du Cloud 3.0

https://www.softwareone.com/fr-fr/
Info.fr@softwareone.com

SOMMAIRE

ÉDITO

Bienvenue dans la nouvelle ère du Cloud 3.0

Mêlant Cloud, collaboration sociale, mobilité, IoT et dorénavant digital Workplace, notre économie digitale a été accélérée mais aussi fortement fragilisée par la crise sanitaire mondiale.
En créant de nouvelles infrastructures, elle a développé de nouvelles vulnérabilités, en se digitalisant, elle a ouvert et fragilisé les réseaux des entreprises, en connectant les objets du quotidien à Internet, elle a invité les cybercriminels directement dans nos salons... Si la dépérimétrisation du réseau favorisée par l'accélération du télétravail a inévitablement exposé les entreprises à une accélération des risques majeurs pour leurs données critiques, le recours au Cloud reste indispensable et continuera de l'être au regard des formidables potentialités et avantages qu'il confère.
Ce livre blanc dresse un état des lieux de l'avancée, de la perception et des principaux enjeux du Cloud pour les entreprises à travers le monde.
Support d'analyse précieux pour les organisations souhaitant accélérer la migration de leurs workloads dans le Nuage, il passe en revue de manière non exhaustive les bonnes pratiques et solutions de sécurité à adopter en se basant sur les évolutions technologiques et les recommandations des instances du marché. Si le choix d'un Cloud hybride reste la solution largement plébiscitée par les organisations pour bénéficier pleinement de l'avantage des deux mondes, sa compréhension et sa sécurité constituent des défis protéiformes qui réclament de la visibilité, de la gouvernance, des solutions technologiques interconnectées et de la responsabilité partagée.

Bonne lecture à tous !

Florent Saussaye,
Cloud Services Lead,
SoftwareONE France

1. LE CLOUD EN FRANCE ET DANS LE MONDE

Cloud hybride ou multiCloud ? Mon cœur balance, ...

A. Le Cloud, accélérateur d'innovations digitales pour l'ensemble du marché mondial

Démocratisation du télétravail, explosion de la collaboration et des opérations à distance, évolution de la relation client-entreprise, boom du e-commerce... autant de bouleversements aussi soudains qu'imprévisibles inhérents à la crise sanitaire. Pour faire face à cette situation sans précédent, les organisations ont accéléré leur transformation digitale et se sont massivement tournées vers le Cloud.
L'enjeu : assurer la continuité de leurs activités stratégiques en donnant accès à leurs données et processus, en tous lieux et à tout moment. Selon Flexera dans son Rapport *State of the Cloud 2021*[1], pas moins de 90% d'entre-elles se seraient appuyées plus que prévu sur le Cloud pour répondre aux nouveaux défis engendrés par la crise.

L'enjeu : *assurer la continuité de leurs activités stratégiques en donnant accès à leurs données et processus, en tous lieux et à tout moment.*

Les différentes typologies de Cloud - Cloud public, Cloud privé, Cloud hybride, multiCloud - permettent en effet de couvrir l'ensemble des besoins et les opportunités proposées semblent aujourd'hui presque illimitées. En témoignent les multiples cas d'usages qui relèvent de la communication, la collaboration, la gestion des processus métiers, le stockage et le traitement de données, la sauvegarde, les tests et développements applicatifs, ou bien encore de l'analytique big data.

Si gagner en agilité et accroître la réactivité ont constitué les principaux moteurs d'adoption du Cloud pendant la crise, les bénéfices tangibles qu'il confère notamment en matière de compétitivité et de personnalisation client sont désormais reconnus par les organisations de toutes tailles et de tous secteurs. Le marché mondial connaît une forte croissance et devrait poursuivre son accélération selon les analystes.
Les dépenses mondiales en matière de Cloud (équipements et services associés) devraient ainsi s'élever à 718 milliards de dollars en 2021 (source IDC). Elles pourraient même dépasser les 1 300 Mrd$ en 2025. Le marché des services Cloud quant à lui devrait atteindre les 400 Mrd$ cette année, dont 385 Mrd$ rien que pour le segment du Cloud public.

En France, le marché des services de Cloud public 2021 est pour sa part estimé à 15,8 Mrd$ selon *Markess by Exaegis*[2].
Il devrait également progresser à hauteur de 19% jusqu'en 2025, tiré notamment par le secteur public (+18%/an) et l'adoption croissante du Cloud par les ETI & PME/PMI, qui pourraient représenter jusqu'à 55% du marché hexagonal en 2025.

CLOUD HYBRIDE, LE CHOIX DES ORGANISATIONS

Retenu par 80% des organisations sondées selon toujours le rapport *State of the Cloud*[1] 2021 de Flexera, le Cloud hybride associe les avantages des environnements de Cloud public (accessibilité, élasticité, intégration) et de Cloud privé (contrôle, sécurité, vitesse), avec une capacité d'orchestration entre les deux plateformes. Cette combinaison offre aux organisations l'opportunité de choisir le Cloud le plus approprié pour chaque application ou workload, mais également de déplacer les charges de travail au gré de l'évolution des coûts et besoins.
Car, si le Cloud privé - dont l'infrastructure et les ressources sont dédiées et accessibles à un client unique - est un environnement idéal pour satisfaire aux exigences de conformité réglementaires et aux besoins de sécurité élevé inhérent au traitement de données sensibles, le Cloud public – un environnement de services partagés entre une multitude de clients dont les ressources et infrastructures sont détenues et gérées par un fournisseur : *le fournisseur de services Cloud* - proposant quant à lui des services élastiques, parfaitement adaptés aux pics et réductions de charges de travail et facturés à l'usage.
Il permet par ailleurs de réduire les dépenses liées aux matériels et infrastructures sur site. En conjuguant ces deux environnements, le Cloud hybride apporte ainsi la souplesse, la sécurité,

[1]https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/
[2]https://www.markess.com/cloud-computing/cloud-francais-un-marche-desormais-pret-a-prendre-son-envol/

la réversibilité et l'adaptabilité requise aux charges de travail et aux usages mouvants des entreprises. Des bénéfices probants qui lui permettent aujourd'hui de s'affirmer en tant que plateforme support de la transformation digitale.

Il est important de noter que le Cloud hybride se distingue des environnements multiCloud. Ces derniers constituent une quatrième typologie d'environnement Cloud reposant sur l'utilisation d'à minima deux Clouds du même type (public ou privé) proposés par différents fournisseurs. Le multiCloud est par ailleurs défini comme hybride lorsqu'une organisation s'appuie sur au moins deux Clouds publics et un Cloud privé.

LES PRINCIPAUX SERVICES PROPOSÉS PAR LE CLOUD TOURNENT AUTOUR DE 3 GRANDES FAMILLES

- **SaaS (Software as a Service).**

Le SaaS est le modèle de distribution logicielle dans lequel les applications sont hébergées par une société ou un fournisseur de services et mises à disposition de l'utilisateur par Internet.

- **PaaS (Platform as a Service).**

Le modèle PaaS permet à un fournisseur Cloud de délivrer les outils logiciels et matériels nécessaires au développement d'applications (langages de programmation, bases de données, ...) en tant que service.

- **IaaS (Infrastructure as a Service).**

Le modèle IaaS fournit des ressources informatiques virtualisées, le fournisseur hébergeant le matériel, le logiciel, les serveurs, les baies de stockage et autres composants informatiques pour le compte de l'entreprise cliente.

AVANTAGES ET CONTRAINTES DU CLOUD PUBLIC ET PRIVÉ

CLOUD PUBLIC

PLUS

- Évolutivité à la demande
- Réduction des dépenses d'investissement (CAPEX)
- Fiabilité avec des services répartis sur plusieurs datacenters

MOINS

- Moins de contrôle sur la sécurité des données
- Enjeu sur leur localisation / souveraineté
- Augmentation des dépenses opérationnelles (OPEX)

CLOUD PRIVÉ

PLUS

- Sécurité. Les données et applications restent derrière les firewalls de l'entreprise ce qui le rend mieux adapté au traitement ou au stockage de données sensibles
- TCO potentiellement inférieur grâce à une diminution des coûts d'exploitation au fil du temps
- Plus de contrôle et de personnalisation
- Flexibilité. Possibilité de déplacer des données non sensibles vers un Cloud public pour répondre au développement de la demande

MOINS

- Coûts plus élevés. Augmentation des frais d'investissement et d'équipement
- Responsabilité. En matière de gestion du datacenter, du matériel et des logiciels d'entreprise, de la sécurité et de la mise en conformité
- Moins de flexibilité dans la montée et la descente en puissance rapide en fonction des besoins

B. CRM, ERP et outils de collaboration dans le Cloud : le tiercé gagnant

La crise aura incontestablement permis au Cloud de faire ses preuves. Les stratégies s'affinent, les migrations s'accélèrent, les usages se multiplient et les investissements s'intensifient. Mais concrètement, où en sommes-nous ?

La nécessité de personnaliser l'expérience client et de mieux appréhender son parcours dans un environnement ultra-compétitif ont incité les organisations à déployer prioritairement dans le Cloud des applications de CRM (Customer Relationship Management ou gestion de la relation client). Cette tendance devrait par ailleurs se poursuivre si nous nous référons à l'étude 2021 « Vers l'adoption du Cloud, étape par étape[3] » menée par Censuswide pour Colt soulignant que si les applications Cloud de CRM sont aujourd'hui utilisées par 75% des entreprises sondées, elles concerneront également 57% des projets Cloud à venir. Les progiciels de gestion intégré (ERP) se placent quant à elles à la seconde place (66%) et devraient également concerner 54% des projets futurs. Les solutions collaboratives représentent pour leur part, 59% des projets. Par ailleurs, le recours à la téléphonie en mode Cloud a également poursuivi sa montée en puissance favorisée également par le travail à distance.

DES BUDGETS SUBSTANTIELS DÉDIÉS À LA MIGRATION DES APPLICATIONS VERS LE CLOUD

Fortes de leurs expériences précédentes, les organisations consacrent désormais des budgets conséquents à la migration de leurs applications vers le Cloud. Selon la même étude Colt, 83% envisageraient d'y investir plus de 100 K€. Si la majeure partie des budgets tourneront plutôt entre 100 et 500 K€, elles sont 21% à souhaiter investir plus de 500 K€.

LE MODÈLE SAAS, EN TÊTE DES STRATÉGIES DE MIGRATION VERS LE CLOUD

Le SaaS s'est développé dans de multiples domaines : suites de productivité (Office 365, G Suite, …), gestion RH, gestion financière, gestion de la chaîne logistique, CRM… et a permis aux télétravailleurs de s'appuyer à distance sur tous les outils nécessaires à leurs activités. 66% des entreprises ont déjà adopté le SaaS dans leur stratégie Cloud tandis que 53% d'entre elles ont aussi basculé vers l'IaaS ou le PaaS (44%) pour développer leurs nouveaux services digitaux.

Les API s'imposent également sans conteste comme l'une des technologies majeures du Cloud. Elles offrent notamment aux organisations et à leurs écosystèmes, la possibilité d'échanger des informations en toute sécurité, mais également d'innover pour accélérer leur croissance. Les technologies de Edge computing (47%) - qui offrent une réelle complémentarité au Cloud pour le stockage de données et de calcul de proximité – ainsi que l'intelligence artificielle (43%) – qui, associée au Cloud, décuple les possibilités en matière de gestion et d'analyses de volumes de datas immenses - contribuent également à soutenir fortement les organisations dans leurs déploiements.

C. Technologies : le socle du Cloud

Le Cloud est porté par de nombreuses évolutions technologiques qui optimisent et complètent les services qu'il délivre. L'Edge computing, le SASE, les API, le SD-Wan, l'IA, le DevSecOps, ou bien encore la conteneurisation, constituent autant de technologies novatrices qui accompagnent son développement.

LE SASE (SECURE ACCESS SERVICE EDGE)

Initié par Gartner en 2019, le SASE est un service d'accès à distance sécurisé qui offre toutes les fonctions de réseau et de sécurité requises grâce à une architecture 100% Cloud. Dans les faits, le SASE raccorde un réseau d'entreprise (type SD-WAN) à divers services de sécurité réseau tels que le ZTNA (Zero-Trust Network Access), des Web Gateways (passerelles web sécurisées), un CASB (Cloud Access Security Broker) et une console d'administration centrale située dans le Cloud.
Cette architecture 100% Cloud permet de sécuriser le trafic entre l'utilisateur et l'application, indépendamment de sa position géographique et du site d'hébergement de l'application. Selon l'enquête européenne Atomik Research pour Zscaler « State of Digital Transformation EMEA 2020[4] », 55% des entreprises prévoient d'adopter une approche SASE, via une migration complète (36%), ou progressive (19%). Le marché du SASE dans son ensemble est évalué à 5,1 Mrd$ d'ici 2024 selon l'étude 2020 de Dell'Oro Group.

L'EDGE COMPUTING

Selon IDC, le marché mondial du Edge computing - définit en tant que réseau maillé de micro-datacenters capables de traiter ou de stocker des données localement - devrait atteindre 250,6 Mrd$ en 2024 avec un taux de croissance annuel composé (TCAC) de 12,5% entre 2019 et 2024. Dopée par l'arrivée de la 5G, cette architecture informatique distribuée pour le traitement des données directement sur les objets ou appareils connectés ou à leur périphérie connaît une forte accélération. L'Edge computing offre l'opportunité de gérer le calcul et le stockage de données à proximité immédiate de l'endroit où elles sont générées. A la clé, un contrôle des données optimisé, une réduction des coûts et des informations obtenues plus rapidement pour une prise de décision accélérée. Avec la multitude de données générées par l'ensemble des objets connectés, l'Edge computing permet d'effectuer un premier traitement des

[3] https://www.colt.net/fr/go/cloud-research-report/
[4] https://www.zscaler.fr/blogs/security-research/state-digital-transformation-emea-increase-remote-work-increasing-risk

données. Les datas nécessitant des analyses plus complexes et donc une plus grande puissance de calcul, peuvent quant à elles être transférées dans le Cloud.

LES API (APPLICATION PROGRAMMING INTERFACE) est un ensemble de protocoles qui simplifie la création et l'intégration de logiciels d'applications. Une API a ainsi pour vocation de faciliter l'intégration par les développeurs de nouveaux composants d'applications dans une architecture existante mais également d'optimiser la collaboration entre les équipes informatiques et métier. Dans un environnement toujours plus compétitif et stimulant, les organisations ont besoin de favoriser le développement et le déploiement rapide de services innovants. Le développement d'applications Cloud-native, conçues pour offrir une expérience cohérente de développement et de gestion automatisée dans les Clouds publics, privés et hybrides, accélère la vitesse de développement. Les API permettent ainsi de connecter aisément l'infrastructure d'une organisation au travers d'applications Cloud native.

LE SD WAN (SOFTWARE-DEFINED WIDE-AREA NETWORK) ouvre de nouveaux horizons en matière de gestion des réseaux. Cette architecture WAN virtuelle offre l'opportunité d'associer les divers services de transport (dont le MPLS et le LTE) et les services d'internet haut débit afin de connecter, en toute sécurité, les utilisateurs aux applications. Le SD-Wan se caractérise notamment par une intégration transparente et une gestion centralisée des technologies et infrastructures de transport permettant de réduire les coûts d'exploitation et de préserver les performances des applications, tout en offrant un haut niveau de sécurité. Il confère de fait un accès simple et rapide à toutes les applications critiques dans le Cloud. Selon Gartner, 65% des organisations auront mis en œuvre le SD-Wan d'ici 2025 afin d'améliorer l'agilité et la prise en charge des applications Cloud.

Autant de technologies novatrices qui accompagnent le développement du Cloud.

L'INTELLIGENCE ARTIFICIELLE (IA)

L'exploitation des données est devenue une composante essentielle de la compétitivité des entreprises. Optimisation de la gestion des organisations, prises de décisions éclairées ou encore meilleur contrôle des systèmes d'information sont autant d'avantages conférés. Pour réussir à manipuler ces immenses volumes de données, l'IA s'est imposée comme une technologie incontournable. Associée au Cloud, elle offre des opportunités sans précédent pour gérer et analyser rapidement et avec précision, l'ensemble des données à disposition. Si l'alliance de l'IA et des technologies Cloud a longtemps été réservée aux grandes entreprises, de nombreux fournisseurs Cloud proposent aujourd'hui des offres adaptées aux ETI et PME. Selon leur maturité et besoins, les entreprises de toutes tailles ont désormais l'opportunité de bénéficier de plateformes de calculs sur lesquelles elles peuvent déposer leurs données et algorithmes, ou plus simplement de s'appuyer sur les services packagés des Cloud providers afin d'exploiter de l'IA pour assurer le maintien de leur compétitivité. Selon le dernier rapport d'IDC, le marché mondial de l'intelligence artificielle en entreprise devrait franchir la barre des 500 Mrd$ d'ici 2024, avec un taux de croissance annuel de 17,5% sur cinq ans. L'étude *Global AI adoption Index 2021*[5] de Morning Consult pour IBM, souligne quant à elle que 40% des professionnels français qui déploient actuellement l'IA prévoient d'investir dans des solutions prêtes à l'emploi.

L'APPROCHE DEVSECOPS vise à enrichir l'approche DevOps en automatisant l'intégration de la sécurité à chaque étape du cycle de vie du développement logiciel, de la conception initiale à la distribution en passant par l'intégration, les tests et le déploiement. In fine, l'approche DevSecOps accélère la livraison de logiciels en offrant l'opportunité aux équipes de développement de fournir plus rapidement un code de meilleure qualité tout en réduisant les risques inhérents à la sécurité. Un enjeu majeur pour faire face à l'explosion des cyberattaques ciblant les vulnérabilités logicielles et accompagner la conversion du déploiement et du développement d'applications aux services Cloud. Selon l'étude « the 2021 State of DevSecOps » de Security Compass, 75% des grandes entreprises sondées (CA > 1 Mrd$ annuel) déclarent suivre une approche DevSecOps afin de gérer proactivement les problématiques de cybersécurité et de conformité réglementaires.

LES CONTENEURS OFFRENT quant à eux un espace d'exécution pour tester des applications en développement et des logiciels. Un conteneur encapsule le code, les configurations ainsi que toutes les dépendances d'une application. Cette technologie permet ainsi d'exécuter une application de manière uniforme, cohérente et rapide sur n'importe environnement informatique. Ainsi, quelle que soit l'infrastructure, les logiciels en conteneur s'exécutent toujours de manière identique.

Eliminant le recours à un système d'exploitation complet pour chaque application, la conteneurisation confère de nombreux avantages tels que la portabilité, l'agilité, l'isolation des erreurs, la simplicité de gestion ou bien encore la sécurité. Selon les dernières prévisions de Gartner, le chiffre d'affaires mondial de la gestion des conteneurs devrait atteindre 944 M$ en 2024.

Parmi les différents sous-segments, l'orchestration de conteneurs dans le Cloud public et les offres de conteneurs sans serveur pourraient connaître la plus forte croissance.

[5] *https://filecache.mediaroom.com/mr5mr_ibmnewsroom/191468/IBM%27s%20Global%20AI%20Adoption%20Index%202021_Executive-Summary.pdf*

D. Le Cloud fait encore peur

Malgré tous ses bénéfices, le Cloud n'en reste pas moins complexe et son adoption globale est encore loin d'être acquise.

FREIN N°1. LA SÉCURITÉ

Les études de marché sont unanimes. Les problématiques de sécurité constituent l'un des enjeux les plus prégnants en matière d'infrastructures Cloud. **La dispersion des charges de travail a étendu les surfaces d'attaques et les menaces peuvent aussi bien provenir d'une erreur humaine, d'un mauvais contrôle utilisateur que de malversations de cybercriminels.** A cela s'ajoutent les problématiques de gouvernance et de conformité, notamment pour les entreprises européennes, confrontées à de nouvelles obligations en matière de souveraineté digitale avec le RGPD (Règlement Général sur la Protection des Données).

37,16% des organisations sondées dans le cadre de l'étude « Global Cloud Survey 2021[6] » de Denodo ont ainsi déclaré que la sécurité, la gouvernance et la conformité constituent des préoccupations majeures en matière de Cloud (vs 32,74% en 2020).

FREIN N°2. LES PROBLÈMES DE COMPATIBILITÉ

Les architectures legacy de certaines entreprises peuvent également perturber cette évolution. Ces systèmes hérités ont hébergé des applications métiers et des données sensibles pendant de nombreuses années. Dans les grandes entreprises, ces environnements sont complexes et les applications sur site se comptent à minima par centaines. Initier ou poursuivre leur migration vers un modèle Cloud s'avère à ce titre souvent délicat.

34% des entreprises estiment ainsi que les architectures legacy complexifient leur adoption du Cloud. *Ever-ready for every opportunity Accenture[7].*

Parmi les autres freins rencontrés par les organisations, on peut notamment citer la complexité des charges opérationnelles, le désalignement entre les métiers et l'IT, les problématiques de gestion du multiCloud, ou bien encore tout simplement les questions économiques. Enfin, le manque de compétences internes semble également impacter de plus en plus d'organisations.

Les études de marché sont unanimes. *Les problématiques de sécurité constituent l'un des enjeux les plus prégnants en matière d'infrastructures Cloud.*

[6] *https://www.denodo.com/fr/document/livre-blanc/denodo-global-cloud-survey-2021*

[7] *https://www.accenture.com/us-en/insights/cloud/_acnmedia/Thought-Leadership-Assets/Images/future-cloud/Accenture-Unleashing-Competitiveness-on-the-Cloud-Continuum.pdf*

2. LA SÉCURITÉ DU CLOUD, UN DÉFI PROTÉIFORME SUR FOND DE PROCESS, DE TECHNOLOGIES ET DE RESPONSABILITÉ PARTAGÉE

Pour les analystes du Gartner, les DSI doivent changer de postulat : ne plus penser « Le Cloud n'est pas sécurisé » mais « Est-ce que le Cloud est utilisé en toute sécurité par mon organisation ? »

A. Une crise rythmée par les cyberattaques

Le constat est sans appel. Les cybercriminels ont profité de la crise sanitaire et de ses effets pour multiplier leurs attaques à travers le monde.
La généralisation du télétravail et du Cloud, aussi massives que rapides, leur ont ouvert la voie à de nombreuses failles de sécurité. Une aubaine pour des cybercriminels toujours plus organisés, ingénieux et offensifs.

En 2020, l'Agence Nationale de la Sécurité des Systèmes d'Information et autorité nationale en matière de sécurité et de défense des SI a recensé 2287 signalements (soit approximativement 6 par jour), dont 759 réels incidents. Dans le même temps, l'organisme a traité 4 fois plus d'attaques par rançongiciels qu'en 2019.
La plateforme cybermalveillance.gouv.fr a, quant à elle, vu sa fréquentation augmenter de 155%, avec plus de 12 000 requêtes émanant d'entreprises, de collectivités ou d'administrations. Le nombre de menaces externes visant des services Cloud a augmenté de 630% entre janvier et avril 2020 *(« Rapport sur l'adoption du Cloud et les risques associés[8] » McAfee).*

Et aucun secteur ne semble épargné. Si les établissements hospitaliers et les biotech ont été bombardés d'attaques pendant la pandémie, les ESN, les administrations, les collectivités, les multinationales comme les PME/PMI et ETI ont également subi une, voire plusieurs cyber-attaques, dont l'actualité s'est faite l'écho.

PORTRAIT-ROBOT DES ATTAQUES ET DES MENACES DANS LE CLOUD

LES ATTAQUES DDOS ou attaques par déni de services, visent le plus souvent à inonder un site web de multiples requêtes simultanées afin de le faire planter. Sur le 1er semestre 2021, Imperva note que ces dernières deviennent de plus en plus courtes (6 min en moyenne), pointues et persistantes.
Elles seraient, de surcroit, utilisées majoritairement pour perturber les équipes réseau et permettre aux cyber assaillants de s'infiltrer en profondeur dans les réseaux des organisations en vue d'exfiltrer des données ou d'installer des logiciels malveillants.

LES MENACES PERSISTANTES AVANCÉES (APT) visent à accéder au réseau d'une organisation en passant sous les radars le plus longtemps possible afin d'épier l'activité dudit réseau et de dérober des données sur une longue période. Compte tenu des moyens nécessaires pour mener une telle attaque, elles ciblent le plus souvent des États et des grandes entreprises.

[8] *https://www.mcafee.com/enterprise/fr-fr/resources/cloud-report.html*

LES INITIÉS MALVEILLANTS, tels qu'un collaborateur ou un prestataire appâté par le gain ou souhaitant simplement nuire à une organisation qui ont accès aux systèmes d'information, mots de passe, données, ou réseau, peuvent également constituer une menace plus que sérieuse.

LES API NON OU MAL SÉCURISÉES

Les API représentent une menace importante pour les entreprises utilisatrices. Gartner estime que d'ici 2022, les attaques contre les API deviendront le vecteur d'attaque le plus fréquent, entraînant des violations de données pour les applications web des entreprises.

LES ATTAQUES ZÉRO-DAY

Elles consistent à s'appuyer sur une faille d'exploitation zéro-day (vulnérabilité logicielle ou matérielle détectée par le cybercriminel avant le fournisseur) pour infiltrer les réseaux et usurper des données.

LES MALWARES (RANSOMWARE, LOGICIELS ESPIONS, CHEVAUX DE TROIE…)

Pas moins de 68% des malwares proviendraient d'applications Cloud et 66,4% d'entre eux seraient initiés à partir d'applications de stockage (type Dropbox, OneDrive…) dans le Cloud. « *Cloud and Threat report*[9] » 2021 Netskope.
Les applications dédiées à la collaboration et les outils de développement constituent la seconde source de malware au 1er trimestre 2021.

Cette liste est loin d'être exhaustive, mais elle laisse présager de l'étendue des menaces auxquelles sont soumises les organisations de tous types à travers le monde. Indéniablement, la sécurité est l'affaire de tous. Elle doit être envisagée dans sa globalité pour sécuriser les actifs et les charges de travail dans le Cloud.

La sécurité est l'affaire de tous.
Elle doit être envisagée dans sa globalité pour sécuriser les actifs et les charges de travail dans le Cloud.

[9] *https://www.netskope.com/lp-cloud-and-threat-report-july-2021-edition-web*

B. Constats et recommandations de l'ANSSI

Les menaces qui pèsent sur le Cloud peuvent être lourdes de conséquences. L'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information (*https://www.ssi.gouv.fr/*) au travers de son centre de Cyber Défense observe différentes lacunes de sécurité au sein des entreprises qui accroissent les surfaces d'attaques. Afin de les soutenir dans cette démarche, le référentiel SecNumCloud, leur offre l'opportunité de distinguer les fournisseurs de services Cloud appliquant les bonnes pratiques en matière de sécurité et propose différentes recommandations pour concrétiser leur projet.

LES LACUNES IDENTIFIÉES PAR L'ANSSI

- Des correctifs de sécurité non appliqués sur les systèmes et les applications,
- Des mots de passe trop évidents ou rarement modifiés,
- Un manque de cloisonnement entre les usages des utilisateurs et des administrateurs réseaux,
- Une gestion trop légère des droits d'accès,
- Une absence de surveillance des SI,
- Une séparation imparfaite des systèmes facilitant la propagation des attaques au sein des réseaux,
- Des accès aux périphériques trop ouverts avec l'usage de clés USB par exemple,
- Un nombre démesuré d'accès externes incontrôlés au SI,
- Un déficit de sensibilisation et de maturité à tous les niveaux hiérarchiques face aux risques encourus.

Ces carences, encore trop régulièrement observées, constituent d'importantes failles de sécurité. Etablir des politiques et des processus sécuritaires précis, en informer l'ensemble des collaborateurs et les sensibiliser sont autant d'éléments contribuant à l'optimisation de la posture de sécurité de l'entreprise.

Mais au-delà de leur propre périmètre d'actions, les organisations doivent également pouvoir s'appuyer sur leur prestataire de services Cloud pour garantir leur sécurité.

LE RÉFÉRENTIEL SECNUMCLOUD, UN CHOIX ÉCLAIRÉ EN MATIÈRE DE FOURNISSEUR DE SERVICES CLOUD

SecNumCloud est une qualification visant à évaluer le niveau de sécurité offert par les prestataires de services Cloud et ce, quelle que soit la typologie de services proposée (SaaS, PaaS, IaaS). Ce référentiel repose sur la norme ISO 27001 - qui spécifie les exigences et bonnes pratiques dans le domaine de la sécurité des systèmes d'information - et intègre des impératifs supplémentaires requis pour les fournisseurs de service Cloud. Les fournisseurs bénéficiant de cette qualification attestent ainsi que leur offre est conforme aux bonnes pratiques énumérées dans le référentiel et que la conformité de leur système a été reconnue par des prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés par l'ANSSI.

La liste exhaustive des fournisseurs de service Cloud qualifiés ainsi qu'une liste partielle des prestataires candidats à cette qualification sont mises à disposition sur le site de l'ANSSI.

LES RECOMMANDATIONS DE L'ANSSI

L'ANSSI apporte également différentes recommandations complémentaires destinées à accompagner les organisations dans leurs projets Cloud, parmi lesquelles :

- **Choisir un prestataire qualifié et exiger que la prestation soit clairement qualifiée :** en se référant à la liste des prestataires qualifiés mise à disposition par l'ANSSI (*https ://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf*), les entreprises sont assurées de contracter avec un fournisseur de services Cloud offrant des services conformes à l'intégralité des exigences du référentiel. Cependant, sachant qu'un prestataire qualifié peut également réaliser des prestations non qualifiées, l'ANSSI recommande d'imposer au fournisseur de services qu'il mentionne dans la convention de service, que la prestation réalisée est effectivement une prestation qualifiée.
- **Capitaliser sur des outils et services qualifiés :** l'ANSSI met à disposition un guide d'achat des produits de sécurité et des services de confiance ayant également fait l'objet d'une qualification. Elle recommande aux organisations de s'y référer pour concrétiser leurs investissements.
- **S'appuyer et suivre les « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing » éditées par la CNIL (*https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf*) et qui couvrent les points suivants :**
  - L'identification des données et des traitements qui migreront dans le Cloud
  - La définition de ses propres exigences de sécurité technique et juridique
  - La conduite d'une analyse de risques afin d'identifier les mesures de sécurité essentielles pour l'entreprise
  - L'identification du type de Cloud pertinent pour le traitement envisagé
  - Le choix d'un prestataire présentant des garanties suffisantes
  - La révision de la politique de sécurité interne
  - La surveillance des évolutions dans le temps

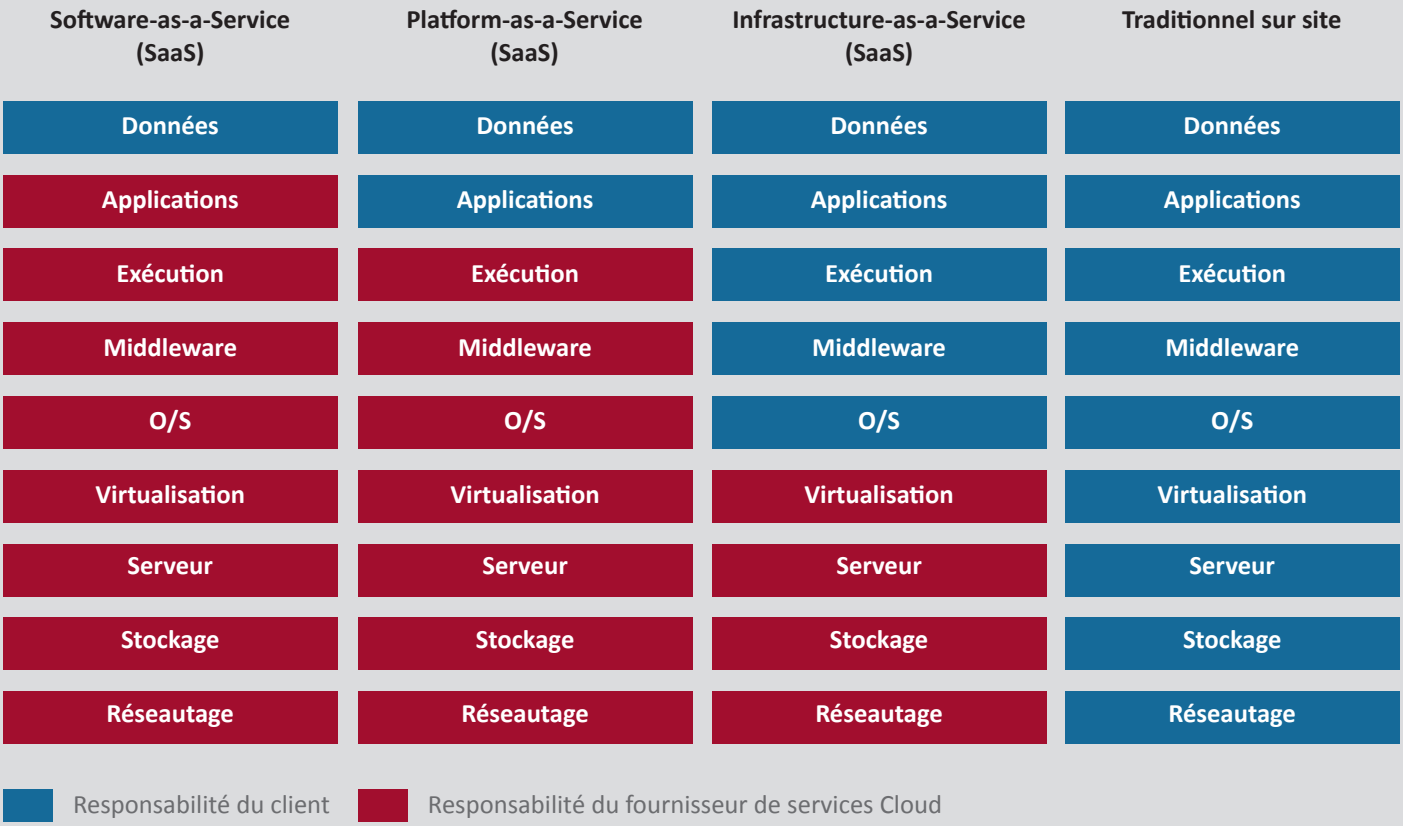
C. La notion de responsabilité partagée avec les fournisseurs de services Cloud

La sécurité dans le Cloud est un enjeu stratégique qui nécessite une protection aux niveaux de l'infrastructure physique, de l'infrastructure virtuelle, des applications et micro-services, de l'identité des utilisateurs et des administrateurs et bien entendu au niveau des données.

Si le sujet peut sembler vaste et complexe, la responsabilité de la sécurité en matière de Cloud n'incombe pas uniquement aux organisations clientes. Elle est pleinement partagée avec le fournisseur de services Cloud.

Ainsi, le cumul des responsabilités relevant à chacun permet d'interagir comme une structure unifiée pour garantir une sécurité optimum, sous réserve de bien choisir également son fournisseur de services Cloud.

La responsabilité partagée permet de définir, en fonction de chaque typologie de service Cloud (SaaS, PaaS et IaaS), le champ des responsabilités de la gestion et de la sécurité entre le client et le fournisseur de services Cloud tel que défini dans le schéma ci-après :



Si le modèle IaaS, confère uniquement au fournisseur de services Cloud la responsabilité de l'infrastructure inhérente au Cloud et sa sécurité, seules les données sont sous la responsabilité du client dans le modèle SaaS. Le fournisseur de services Cloud assure de fait une grande partie de la sécurité dans le SaaS. Le PaaS, quant à lui, confère la responsabilité des infrastructures virtuelles au fournisseur de services Cloud.

Dans ce cadre, le fournisseur de services Cloud doit être à même de proposer toute une palette de services permettant d'accompagner les organisations dans la gestion de leur stratégie, de leurs politiques et de leurs contrôles de sécurité dans le Cloud. Et nombre d'entre elles s'orientent désormais vers des environnements de Cloud hybride.

LA VISIBILITÉ ET LE CONTRÔLE, DES AXES DÉTERMINANTS DANS LE CHOIX D'UN FOURNISSEUR DE SERVICES CLOUD

Les organisations doivent réussir à établir une approche de sécurité homogène au sein de leurs environnements Cloud. Dans certains cas, l'organisation ne dispose pas d'une visibilité exhaustive de sa sécurité. Elle a donc besoin de bien comprendre la façon dont le Cloud va affecter son profil de risque ainsi que l'intégrité de ses données, les questions de vie privée et la disponibilité de ses activités. Les fournisseurs de services Cloud doivent être à même de leur offrir une visibilité permanente et l'opportunité de gérer efficacement l'ensemble des contrôles dans leur écosystème Cloud.
Ainsi, lorsque les organisations sont en passe de sélectionner leur fournisseur de services Cloud, elles doivent également s'interroger sur sa capacité à les accompagner sur l'intégralité de leurs enjeux sécuritaires.

D. Comment garantir une bonne protection

ADOPTER UNE GOUVERNANCE DE LA SÉCURITÉ ET DE L'INFORMATION

En mai 2020, Blackbaud, un fournisseur de services dans le Cloud a pu arrêter une attaque de ransomware cherchant à crypter des fichiers confidentiels mais hélas sans éviter le paiement d'une rançon pour empêcher la fuite en ligne des données de ses clients.
De son côté, la même année, AWS a encaissé la plus grande attaque DdoS de son histoire de l'ordre de 2,3 Tb/s tandis que au sein de General Electrics une personne non autorisée a pu facilement accéder et dérober les informations d'identification personnelles de ses collaborateurs.

Pourquoi ces attaques ont-elles réussi ? Comme nous l'avons vu, les causes peuvent êtres multiples : les politiques de sécurité n'ont pas été appliquées correctement, des failles de sécurité ont été générées impliquant trop d'accès à privilèges ou encore un des acteurs responsables en matière de protection des données avec le fournisseur de services Cloud a fait preuve de défaillance.
On peut également évoquer sans trop se tromper un manque de visibilité sur l'ensemble des services Cloud à l'échelle de l'organisation ou encore une mauvaise configuration des infrastructures - à l'instar d'une équipe habituée aux environnements on premise qui a pu accidentellement configurer l'accès aux ressources Cloud de manière trop large, créant par là même des failles pour des attaques directes ou des déplacements latéraux. **Gartner confirme que, d'ici 2025, 99% des problèmes liés à la sécurité du Cloud seront le résultat d'une erreur humaine.**

Il est indéniable que l'introduction du Cloud dans une organisation affecte les rôles tout comme les responsabilités et les processus. Sans gouvernance fournissant des directives précises pour gérer les profils de risques, le Cloud produit l'effet inverse que celui escompté et les entreprises se retrouvent souvent avec des projets bloqués, ou non alignés avec leurs objectifs business, des manquements règlementaires, des dépassements budgétaires, et bien plus encore…

Dans un environnement Cloud multi-organisations ou multi-plateformes, les participants s'engagent à promouvoir et à établir des attentes communes en matière de sécurité et de niveaux de service. La gouvernance définira également le processus de réponse à une violation du protocole, et impliquera l'ensemble des décideurs - dont la responsabilité aura au préalable été définie - dans la remédiation et les processus de communications aux instances réglementaires impliquées.

Comme le Cloud expose le patrimoine de données des organisations ; ces dernières devront mettre en place également une gouvernance de l'information pour assurer la bonne maitrise de leurs données. **La gouvernance permettra de déterminer quelles applications seront portées dans le Cloud, segmenter les données en fonction de leur criticité, identifier les objectifs métier et maîtriser les risques**.

Si le respect de la conformité est déjà difficile sur site, le Cloud y ajoute encore une couche de complexité additionnelle. Les outils et pratiques déjà existants dans l'entreprise peuvent parfois complexifier les contrôles sur le Cloud. Par exemple, les organisations fortement régulées qui doivent répondre d'une conformité HIPAA pour les données médicales doivent identifier à tout moment où ces données sont stockées, déplacées ou consultables dans le Cloud.
Il est donc nécessaire de bien comprendre le fonctionnement du Cloud et identifier la localisation de ses données tout en mettant en place encore une fois des contrôles avec les principaux fournisseurs de Cloud pour satisfaire aux exigences règlementaires locales et aux enjeux de souveraineté.

MAIS QU'ENTENDONS-NOUS PAR GOUVERNANCE DE LA SÉCURITÉ DU CLOUD ?

La gouvernance de la sécurité du Cloud est un ensemble de politiques et de normes qui facilite la gestion et des opérations de sécurité efficaces dans l'environnement Cloud en se basant sur une évaluation des risques, des procédures d'audit, de mesure et de reporting, ainsi que l'application des politiques de sécurité dans une logique d'amélioration continue et de responsabilité partagée.

UNE VISION 360 POUR ÉLIMINER LES ANGLES MORTS

La plupart des organisations n'ont pas de visibilité suffisante sur ce qui se passe dans leur infrastructure Cloud. Dans un contexte où elles gèrent souvent un environnement multiCloud - SaaS, PaaS, Cloud privé et solutions sur site - cela implique ainsi d'avoir une compréhension globale à 360 degrés du parc et des compétences requises sur les différentes plateformes utilisées. Le Cloud complexifie la visibilité car ses instances virtuelles sont dynamiques et évoluent continuellement. Les pratiques de sécurité traditionnelles sont souvent contournées ou engagées trop tard dans le cycle de déploiement.

En outre, certaines nécessitent une intervention manuelle ou, pire encore, ne prennent pas en charge les contrôles de sécurité Cloud et Cloud natifs. Par conséquent, le service informatique ne peut pas mesurer les risques de manière fiable et à l'échelle de l'organisation. Le passage au Cloud implique d'affiner les pratiques d'évaluation et de gestion des risques. **La sécurité doit être intégrée à tous les niveaux de la pile d'applications et d'infrastructure y compris sur site physique, Cloud privé, Cloud public et micro services, ainsi que dans les processus de développement au sein d'un pipeline d'intégration et de déploiement continus (CI / CD)**. Une approche holistique orientée *Security by Design* qui doit être administrée à travers un tableau de bord unifié pour le multiCloud.

AUTOMATISEZ !

Une mauvaise configuration de la sécurité ou des modifications à y apporter peut conduire à des vulnérabilités système. C'est pourquoi l'automatisation de la sécurité mais aussi des cycles de Patching va permettre de détecter et de corriger de manière proactive les problèmes, permettant une mise en application cohérente des règles de sécurité pour libérer les analystes des tâches rébarbatives. **Il est prouvé que l'automatisation de la sécurité est capable de réduire de 95%, le coût moyen d'une violation mais elle est uniquement appliquée par seulement 16% des organisations selon IBM Security dans son rapport « 2019 Cost of a Data Breach Report !**[10] **».** Les organisations devraient donc investir dans une solution d'automatisation qui minimise les fausses alertes, tout en permettant aux équipes de sécurité d'obtenir une visibilité holistique de leur environnement pour optimiser la posture cyber défense.

UNE STRATÉGIE DE SÉCURITÉ MULTI COUCHES

La sécurité du Cloud nécessite également une stratégie de sécurité multi couches, toutes interconnectées entre elles.

Les organisations ont mis en place une grande variété d'approches et d'outils technologiques en matière de sécurité du Cloud souvent silotés et qui pour beaucoup n'ont pas tenu leurs promesses comme :

- des outils maison (difficiles à maintenir et à mettre en œuvre)
- des solutions technologiques multi fournisseurs (qui fonctionnent de manière indépendante)
- des pare-feu (un échec hors de la sécurité périmétrique)
- des outils de sécurité adaptés uniquement au Cloud (inefficaces pour les environnements hybrides et qui entraînent des silos supplémentaires)

Les environnements multicloud, composés de charges de travail réparties sur diverses instances et fournisseurs de Cloud auxquels s'ajoutent des infrastructures legacy, doivent être protégés par des outils de sécurité capables de fonctionner sur l'ensemble de l'infrastructure hybride et multiCloud et intégrés dans le pipeline CI/CD de développement et d'intégration continus.

APPLIQUER ZERO TRUST ET SASE

Les limites des solutions de sécurité traditionnelles telles que les VPN ou les firewalls dans un contexte de développement du Cloud, du BYOD et du télétravail ont progressivement imposé le framework Zero Trust (ZTNA) sur le marché.

Zero Trust applique à l'accès aux réseaux le principe de sécurité du moindre privilège. Plus précisément, aucun utilisateur ou appareil n'est digne de confiance et de ce fait, ne pourra accéder aux ressources sans autorisation.

C'est, selon l'ANSSI, une modification totale du paradigme de la stricte logique périmétrique qui a longtemps prévalu au sein des entreprises. Pour que ce modèle fonctionne, les organisations doivent vérifier et micro segmenter l'ensemble de leurs ressources, limiter et appliquer des contrôles stricts des accès, mais aussi inspecter et enregistrer tout le trafic réseau en y impliquant à la fois les terminaux, les charges de travail et les données.

Alors que les organisations évoluent vers des environnements toujours plus distribués, la question de l'interconnexion entre ce modèle stratégique de sécurité Zero Trust et le SASE (Secure Access Service Edge) se pose de plus en plus.

Si Zero Trust implique une authentification forte des utilisateurs et l'accès sécurisé aux données et aux systèmes en fonction des ressources dont ils ont besoin, le SASE se focalise lui sur des plateformes de contrôle du réseau à la périphérie du Cloud protégeant les données, partout où elles circulent.

Plateformes intégrées composées d'un ensemble de solutions complémentaires, les offres SASE sont ainsi décisives dans le cadre de l'application d'un modèle Zero Trust pour la protection du Cloud.

[10] *https://www.ibm.com/downloads/cas/RDEQK07R*

CONCLUSION

La crise sanitaire mondiale a exacerbé encore plus l'importance de la résilience, de l'agilité, et de l'évolutivité des systèmes informatiques. S'il est clair que le Cloud, catalyseur de l'innovation et de la croissance, apporte toutes les capacités nécessaires au bon fonctionnement et à la pérennité des organisations, son adoption n'en reste pas moins complexe.

Une migration ne doit pas être précipitée mais s'accompagner d'une stratégie clairement définie notamment sur le choix des applications legacy éligibles à la migration, la compréhension de l'impact sur les métiers ou encore le choix des solutions techniques qui vont permettre de tracer et de protéger les données. Un partenaire de confiance vous apportera toute l'expertise nécessaire à la conduite optimale du projet, de manière agile, dans le respect du cahier des charges et des coûts, et avec un usage optimal des ressources.

À PROPOS

De SoftwareONE

SoftwareONE est un fournisseur mondial de solutions logicielles et Cloud, qui accompagne ses clients dans la réussite de leur transformation digitale avec des services dédiés.
SoftwareONE permet aux organisations de faciliter et accélérer la modernisation de leur infrastructure et de leurs postes de travail, tout en optimisant les actifs logiciels et Cloud associés.

De IBM

IBM est le partenaire de confiance des organisations qui, dans un contexte fortement concurrentiel, doivent se réinventer sans cesse en tirant parti entre autres des plateformes Cloud et des plateformes d'Intelligence Artificielle.

IBM et son écosystème accompagnent ces organisations dans leur transformation pour les aider à rester compétitives, en co-créant des solutions innovantes, en co-développant des business modèles disruptifs, quels que soient les secteurs d'activité concernés.

softwareONE

Gold
Business
Partner

IBM

CONTACTEZ-NOUS SUR

https://www.softwareone.com/fr-fr/
Info.fr@softwareone.com