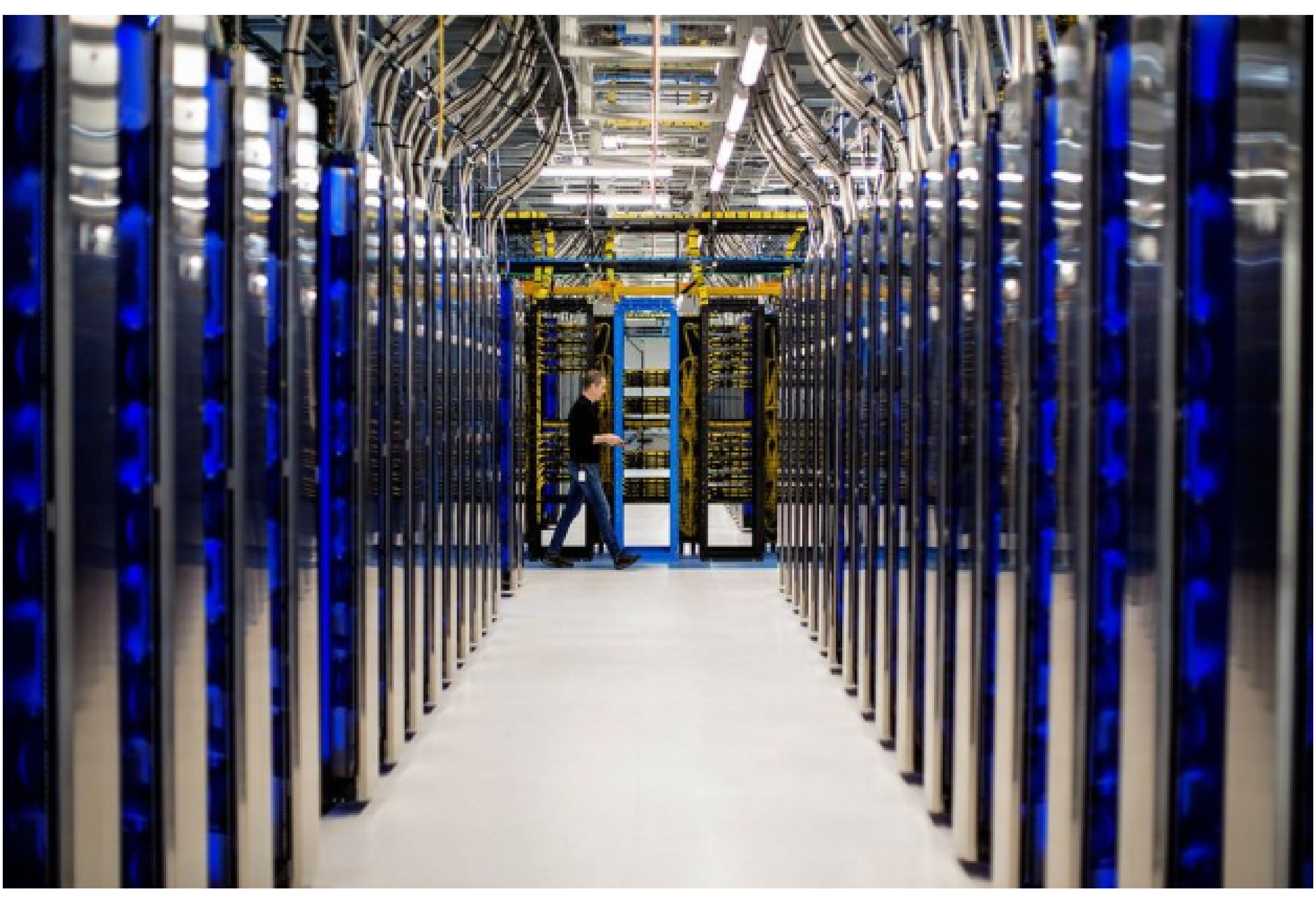
À quel cloud faut-il se fier ?

RIDHA LOUKIL | EDF , THALES , DASSAULT AVIATION , OVH , SÉCURITÉ | PUBLIÉ LE 04/03/2020 À 07H00

ENQUÊTE L'État et l'industrie de la cybersécurité travaillent à l'émergence d'un cloud de confiance. Il en va de la souveraineté digitale de la France et de l'Europe.



Comment faire émerger un cloud de confiance ? © Microsoft

SUR LE MÊME SUJET

"L'Europe doit disposer de ses propres capacités numériques, en informatique quantique, 5G, cybersécurité ou IA", défend Ursula Von der Leyen

TWITTER FACEBOOK LINKEDIN FLIPBOARD EMAIL

Le cloud souverain est mort, vive le cloud de confiance ! Fin janvier, Orange a éteint Cloudwatt, tournant définitivement la page peu glorieuse du cloud souverain. Mais le besoin d'un cloud indépendant, à l'abri d'intrusions de puissances étrangères, n'a pas pour autant disparu. Il s'exprime aujourd'hui sous le nom de cloud de confiance.

Le concept est encore flou. Lancé au début de 2018 par Bruno Le Maire, le ministre de l'Économie, avec la volonté de faire émerger des offres, il fait l'objet d'un projet de développement du contrat conclu entre l'État et la filière stratégique de cybersécurité. Y participent des offreurs de cloud comme OVH, Outscale et Oodrive, mais aussi de grandes entreprises comme Thales, EDF et Docaposte. La première étape consiste à en proposer une définition cette année.

Pas question de reproduire les erreurs du cloud souverain. "*Nous avons retenu les leçons de cet échec,* confie Édouard de Rémur, le cofondateur d'Oodrive et copilote du projet aux côtés de Michel Paulin, le directeur général d'OVH. *Ce projet est plus structuré et plus réfléchi que celui du cloud souverain. Et le fait que l'État et la filière travaillent ensemble change tout. Il y a une volonté commune d'assurer l'indépendance numérique de la France et de l'Europe.*"

Le projet comporte deux volets : l'un technique, l'autre réglementaire. Sur le premier, les clouds américains, qui dominent le marché, ont l'avantage. C'est ce qui explique que de grands groupes comme Airbus, Air liquide, Axa, Veolia, Sanofi, Schneider Electric, Total et la SNCF aillent chez Amazon, Microsoft, Google, IBM et Salesforce. "*Nous voulons, non pas les remplacer, mais les compléter dans les applications sensibles,* souligne Édouard de Rémur. *Nous disposons déjà des différentes briques. L'enjeu est de les agréger dans des solutions intégrées, performantes et compétitives, comme chez les Gafam. Et là où il y a des trous, nous devons soutenir l'émergence d'offres nationales. Tout cela est possible. C'est juste une question de volonté et de mentalités.*" Un catalogue d'offres qualifiées "*de confiance*" est prévu pour 2021.

Prévenir les risques liés au Cloud act

La sécurité est au cœur des réflexions. L'État donne l'exemple. Il a défini ses besoins en trois cercles. D'abord, les données ultrasensibles, qui restent en interne sous son contrôle. Ensuite, les données sensibles, qui peuvent être migrées vers des clouds de confiance. Enfin, les données non sensibles, qui peuvent aller sur le cloud public. "*C'est la bonne approche, déjà en pratique dans les grandes entreprises, car toutes les données n'ont pas la même sensibilité,* estime Gérôme Billois, consultant au cabinet Wavestone. *Il est intelligent de ne pas mettre tous ses œufs dans le même panier. Les questions de confiance se posent même au cercle trois.*"

Un label s'impose comme la consécration de la confiance : SecNumCloud. Il est délivré par l'Agence nationale de la sécurité des systèmes d'information (Anssi). Vu comme un sésame pour les marchés cloud de l'État, des collectivités locales et des opérateurs d'importance vitale, il pourrait devenir une exigence de toutes les entreprises pour leurs données sensibles. Deux acteurs l'ont décroché : Oodrive, fournisseur de services de travail collaboratif, et Outscale, la filiale de cloud d'infrastructure de Dassault Systèmes. D'autres, dont OVH, Cheops Technology et Worldline, y sont candidats.

Le volet réglementaire s'annonce épineux. Le Cloud act promulgué en 2018 aux États-Unis est dans tous les esprits. Cette loi donne au gouvernement accès aux données gérées par les clouds américains même en dehors du pays. Bercy craint qu'elle ne soit détournée de son but affiché – la lutte antiterroriste – et n'ouvre la voie à l'espionnage économique. "*La solution technique existe,* affirme Jean-Noël de Galzain, le PDG de Wallix et président d'Hexatrust. *Elle passe par le cryptage de bout en bout, le contrôle des accès, la gestion des identités et la traçabilité, pour savoir qui accède à quoi et quand. Nous allons construire une solution complète pour le cloud de confiance.*"

Reste la question de l'extraterritorialité du Cloud act. "*Il n'y a pas d'accord bilatéral entre l'Union européenne et les États-Unis,* rappelle Alban Schmutz, le vice-président d'OVH et président de l'association européenne des fournisseurs de cloud d'infrastructure. *L'idéal serait de porter le sujet au niveau multilatéral. Une voie difficile avec Trump.*"

Les promoteurs du cloud de confiance entendent démystifier le Cloud act en menant un travail de sensibilisation des entreprises sur les risques encourus et de clarification des offres sur le marché. Des règles favorisant la réversibilité, la portabilité et la transparence seront établies en 2022. "*Le sujet de l'extraterritorialité des lois américaines doit être pris au sérieux,* assure Alban Schmutz. *Le Cloud act n'est pas compatible avec le RGPD. Le Comité européen de protection des données, qui réunit les Cnil européennes, le dit. Il faut pousser les fournisseurs américains à être transparents, à dire où les données sont stockées, quelle réglementation est applicable et à le préciser dans les appels d'offres. Il faut aussi éduquer les entreprises et les administrations utilisatrices pour qu'elles mettent ces questions sur la table.*"

Des certifications aux labels de confiance

1.Certifications standards

Des certifications selon des standards (ISO 27001, SOC, PCI DSS...) attestent de la mise en place d'un système de management de la sécurité visant à limiter les risques de vol, d'altération ou de perte de données. Si elles offrent un socle minimum de sécurité ou des garanties spécifiques (données financières, données de santé...), elles ne répondent pas aux préoccupations de confiance.

2.Certifications sur mesure

L'entreprise fait elle-même certifier son fournisseur pour s'assurer qu'il respecte ses propres exigences en matière de sécurité et de confidentialité des données. Mais tous les fournisseurs de cloud n'acceptent pas de se prêter à l'exercice ou le font payer par des coûts dissuasifs. Une démarche envisageable pour les grands groupes mais pas pour les ETI ou PME.

3.Labels de confiance

Ils attestent du respect d'un référentiel de sécurité. Le nec plus ultra dans ce domaine est le SecNumCloud délivré par l'Anssi, l'Agence nationale de sécurité des systèmes d'information. Il est vu comme un sésame pour le marché cloud de l'Etat, des collectivités locales, des opérateurs d'importance vitale ou encore les entreprises de services essentiels.

Trois étapes clés

- 2020 Qualification du cloud de confiance selon la sensibilité des données
- 2021 Proposition d'un catalogue d'offres qualifiées "*cloud de confiance*"
- 2022 Adoption de règles de réversibilité, de portabilité et de transparence

Source : Comité stratégique de la filière Industries de sécurité