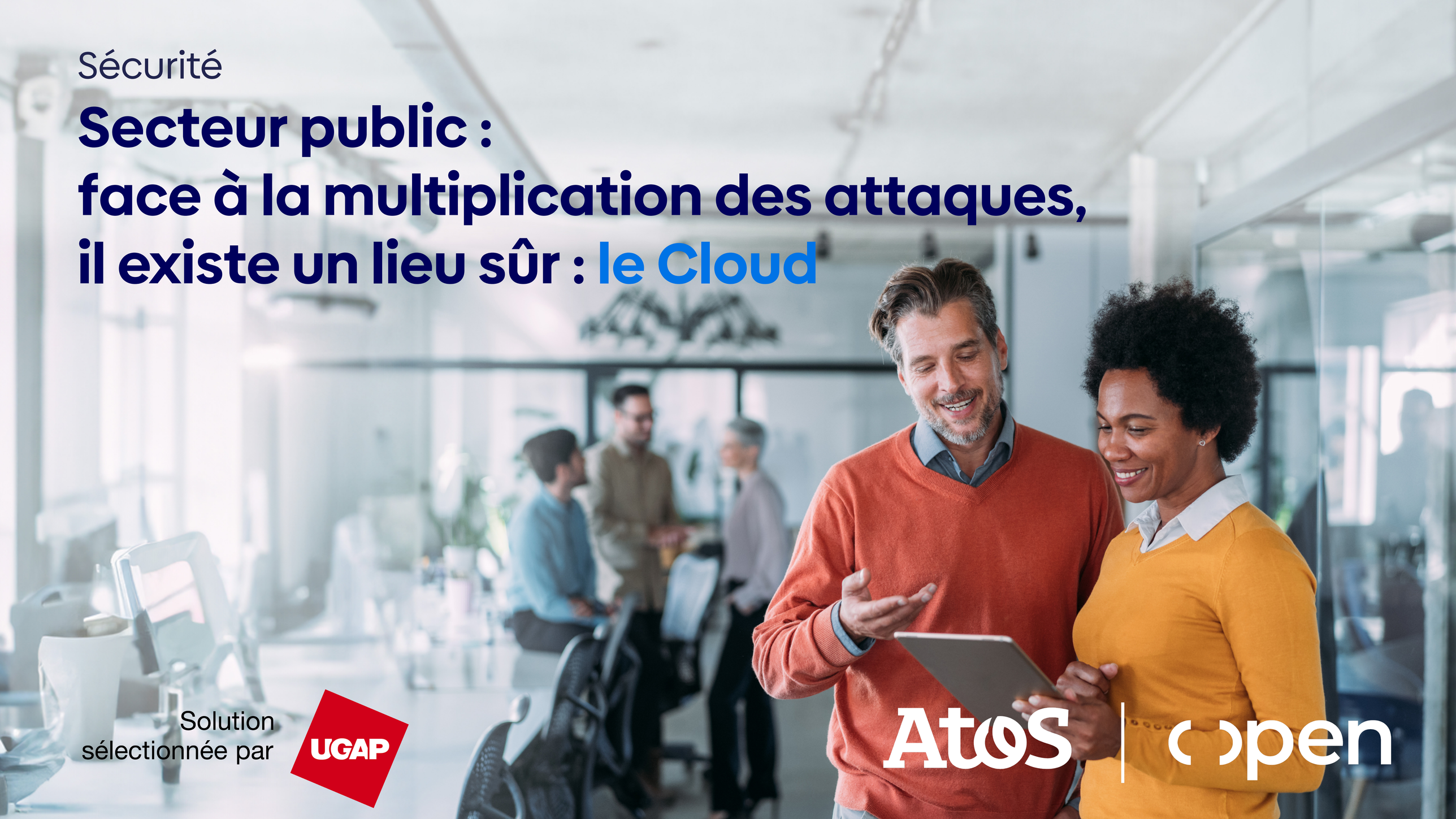
Sécurité

Secteur public : face à la multiplication des attaques, il existe un lieu sûr : le Cloud



Solution sélectionnée par UGAP

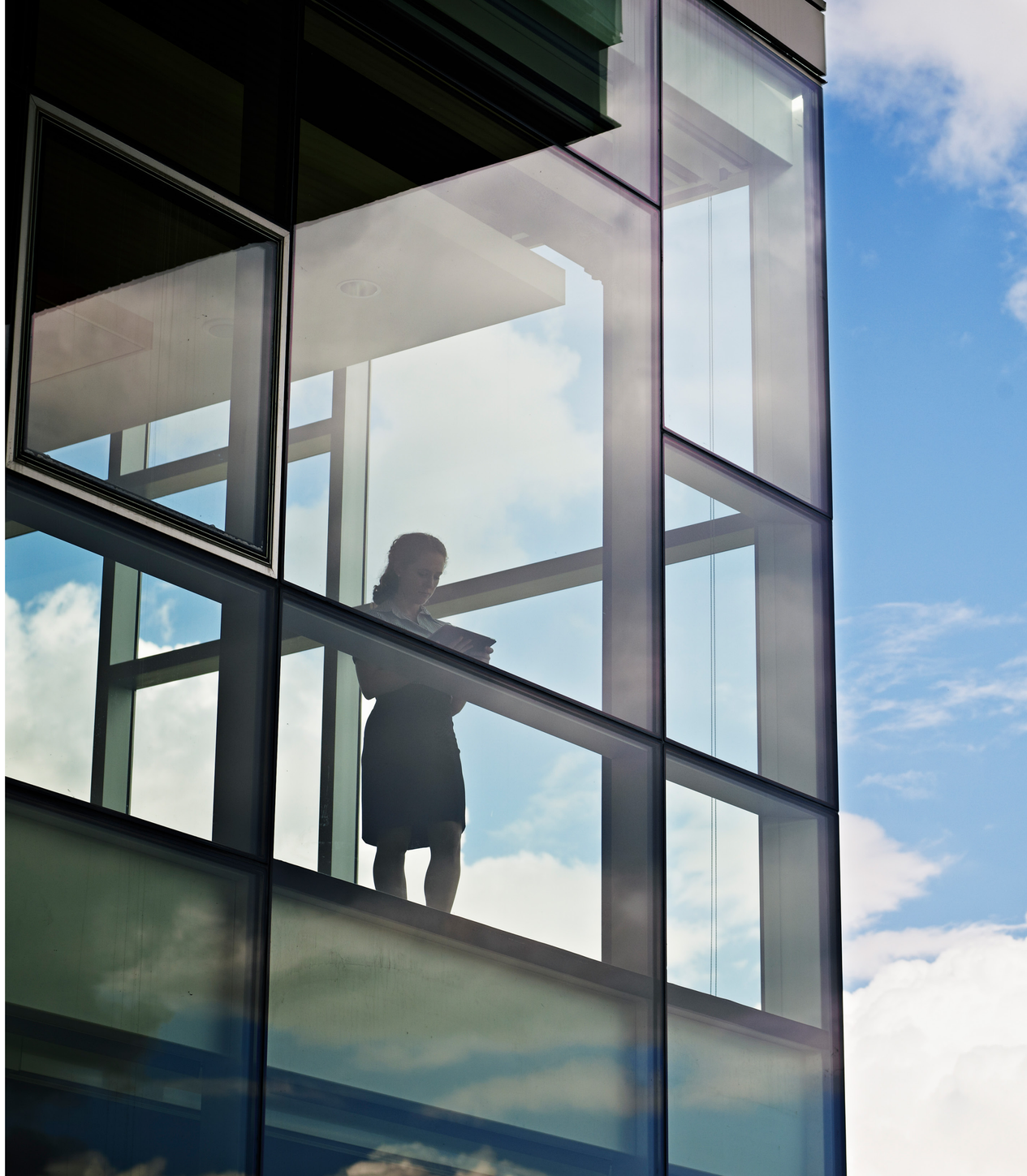
Atos | cloud open

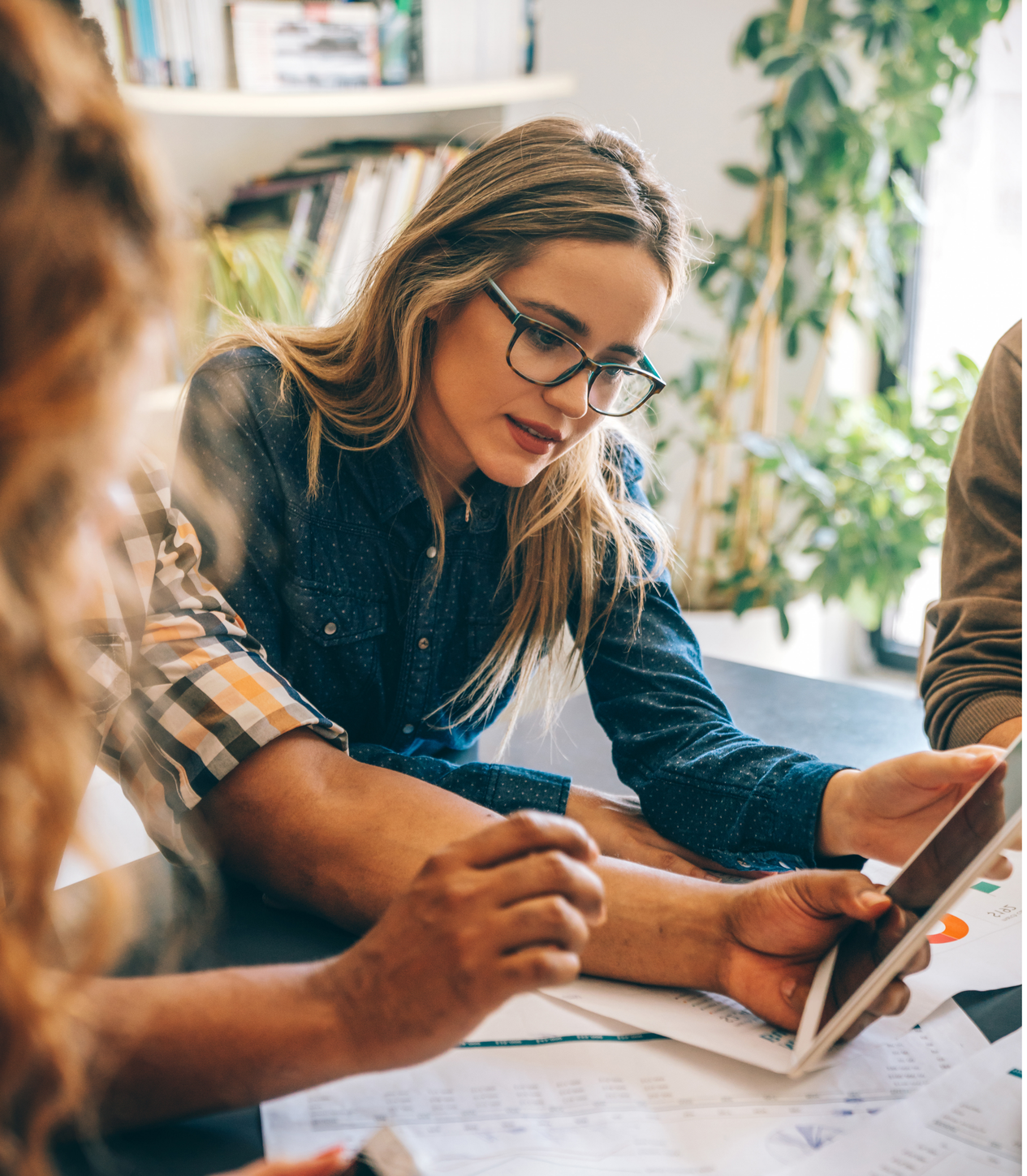
Le Cloud est une révolution pour la modernisation des services de l'Etat français. La doctrine française du « Cloud au centre » est sans ambiguïté : les services de l'État et les organismes placés sous sa tutelle sont fortement incités à utiliser le Cloud comme modalité d'hébergement par défaut pour leurs projets informatiques.

L'Etat fait donc preuve d'une démarche volontariste, en levant tous les freins à l'adoption du Cloud. Cette ambition se matérialise par la mise à disposition de marchés simplifiant la commande publique, notamment par le recours des grandes centrales d'achat de l'Etat comme l'UGAP, ainsi que d'une adaptation du code de la Commande Publique.

7 sur 10 décideurs IT

Dans le monde, presque 70% des décideurs IT s'attendent à être victimes d'une cyber attaque en 2024, selon l'enquête de Statista (www.statista.com).





Bien que conscientes du risque, les organisations du secteur public n'ont à ce jour pas pour autant pu déployer toute leur stratégie en matière de sécurité informatique.

En effet, beaucoup s'interrogent encore sur les enjeux d'une migration vers le Cloud.

Leurs données sont-elles plus sécurisées « sur site » (On Premise) ou sur les serveurs d'un fournisseur Cloud ?

Pour nous, le match est joué d'avance - et le Cloud l'emporte par KO ! Mais il est important d'expliquer pourquoi.

Ce document présente 5 points clés factuels pour vous permettre de trancher.

1. La sécurité et la souveraineté sont deux choses différentes

Attention tout d'abord à ne pas se tromper de combat. Chez nos clients, nous observons souvent une confusion entre **un sujet technique (la sécurité)** et un **sujet géopolitique (la souveraineté)**. Malgré l'essor des offres de nos CSP français et leurs efforts pour un enrichissement permanent, il reste difficile de rivaliser avec les catalogues de services pléthoriques des hyperscalers (issus de milliards de dollars de R&D…).

Le C.L.O.U.D. Act (Clarifying Lawful Overseas Use of Data Act) des Etats-Unis n'a pas été élaboré dans l'optique de permettre un espionnage industriel massif. Bien au contraire, Il s'agit simplement d'un cadre juridique pénal très strict encadrant les demandes d'accès à certaines données dans des contextes graves (crimes et terrorisme notamment). Une loi comme il en existe beaucoup d'autres, y compris en France et en Europe. Mais, répétons-le, ceci est un autre débat !

Cette loi a été très critiquée pour son caractère extraterritorial. Cependant, il existe des raisons de penser que cette menace est limitée. Le Cloud Act[1] prévoit que les fournisseurs de services américains peuvent s'opposer à une demande d'accès aux données si celle-ci violerait la législation du pays dans lequel les données sont stockées. A titre d'exemple, AWS a annoncé avoir reçu pour le 1er semestre 2023 plus de 1 300 demandes dont seules 16 ont abouti. A noter que sur ces 16 dossiers, les demandes n'émanent pas uniquement des Etats-Unis mais d'autres pays comme l'Allemagne, la Grande-Bretagne et la France.

En France, le règlement général sur la protection des données (RGPD) prévoit des garanties importantes pour la protection des données personnelles, ce qui pourrait limiter la possibilité pour les autorités américaines d'accéder aux données des citoyens français.

Pour rappel, les clés de chiffrements sont entre les mains des clients, mais en aucun cas accessibles par le CSP.

Dans le même esprit : être qualifié « SecNumCloud », c'est très bien en termes de souveraineté, toutefois en termes de sécurité cela ne garantit qu'un filet minimum. Un environnement SecNumCloud, par exemple, n'est pas suffisant en termes de sécurité pour héberger une offre bancaire.

[1] Section 103(c)(2)(A) du Cloud Act : « A provider of electronic communications service may not be required to disclose information under this section if the disclosure would be unlawful under the law of the country in which the information is stored.»

2. Faire un état des lieux, c’est faire un pas en avant

Migrer dans le Cloud, cela signifie qu'on remet tout à plat, pour s'interroger sur l'existant : comment les données sont-elles classées aujourd'hui ? Avec quels accès et dans quelles conditions ?

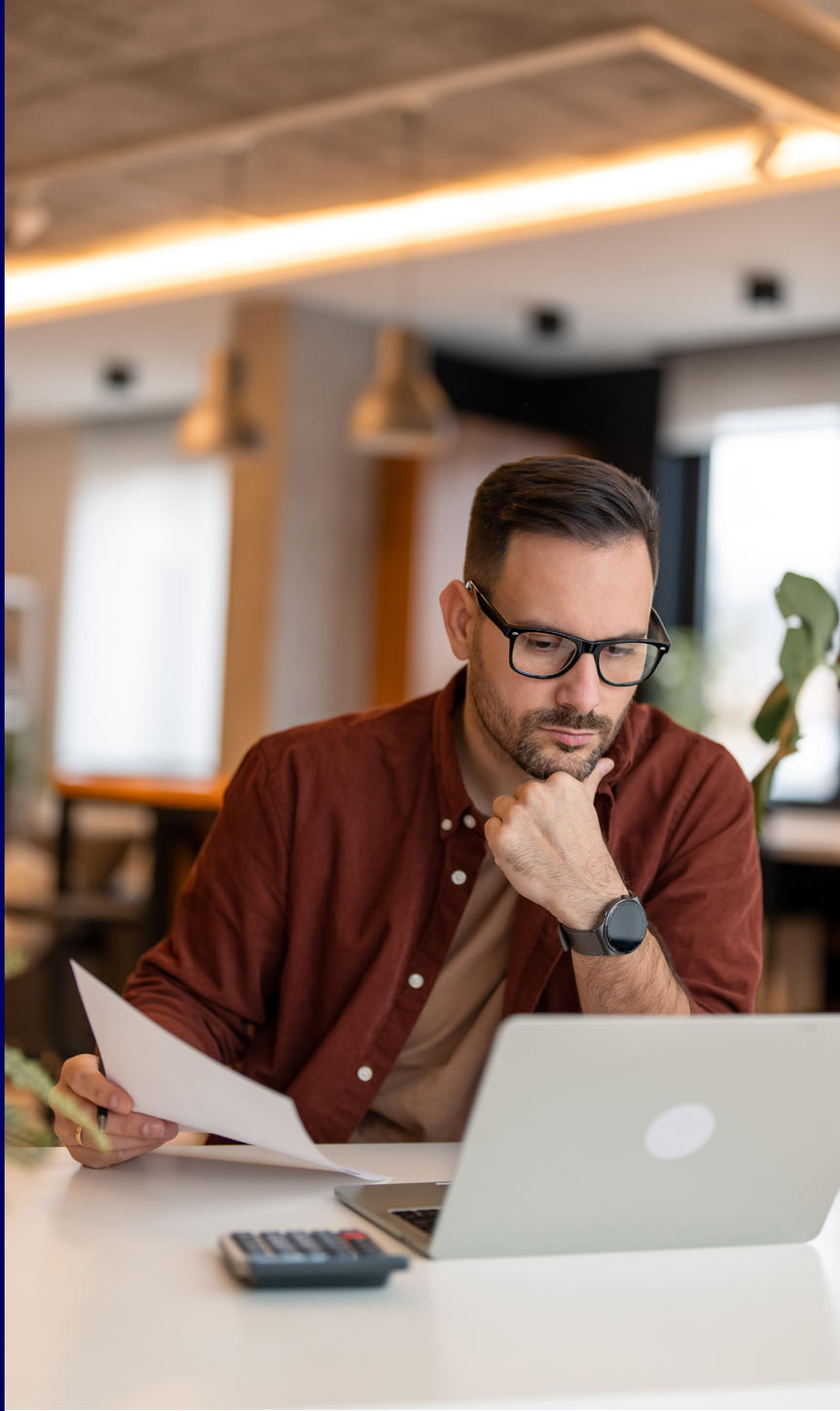
Ce travail d'état des lieux, ainsi que la nécessaire gouvernance à mettre en place autour de la réflexion Cloud, constituent une base très saine.

Vos décisions seront collégiales, incluant jusqu'au DRH et au DAF. Cette façon de faire table rase est, à elle seule, un progrès en matière de sécurité.

Face à la pression de la menace cyber, la Directive européenne **NIS2** (Network and Information Security) marque une nouvelle étape pour renforcer la sécurité des Systèmes d'information. Publiée fin 2022, son entrée en vigueur est prévue en France en octobre 2024, sous le pilotage de l'**ANSSI**. Sa mise en application va permettre aux organisations de mieux se protéger. La directive NIS 2 élargit les objectifs et le périmètre d'application de NIS pour apporter davantage de protection aux systèmes d'information.

Les organisations doivent donc se poser les bonnes questions (Suis-je concerné par cette directive ? Si oui, sur quel périmètre et quelle est la trajectoire à adopter ?) et d'ores et déjà réfléchir à la mise en place de mesures de renforcement de la cybersécurité, comme les plans de continuité (PCA) et la reprise d'activité (PRA).

3. Sécurité et… résilience



Dans un pays comme la France, où l'accès à la santé, l'éducation, ou encore la protection sociale sont de plus en plus digitalisés et accessibles via internet, le cloud est un moyen simple et efficace de garantir la continuité du service public en cas de sinistre touchant les infrastructures ou les données (cyber-attaque, incendie, inondation, panne matérielle…).

La mise en place d'un service de **PRA** (Plan de Reprise d'Activité) dans le cloud permet de basculer un système d'information complet sur un site de secours en quelques heures et garantit l'accès des usagers à des services essentiels. Le cloud devient ainsi une solution centrale dans la recherche de résilience des organisations publiques.

Dans le cas ou votre système d'information a déjà migré dans le cloud, vos données peuvent facilement être répliquées dans plusieurs Data Centers au sein des « Availability Zone » des CSP, constituant elles-mêmes les « Régions » : c'est un gage de résilience. Pensez-vous être parfaitement à jour de vos sauvegardes ? Et à l'inverse, pensez-vous avoir réduit ces copies au strict nécessaire (car plus vous avez de doublons, plus vous avez de surface d'exposition au risque) ?

Autres points : grâce au Cloud, les accès sont mieux gérés, les correctifs sont mis en œuvre bien plus rapidement et le taux de certification / adaptation aux nouvelles normes est inégalable.

Dans notre monde incertain, le Cloud public répond mieux à la variabilité que le "On Premise". Ces éléments sont très importants, car si vous voulez comparer les coûts d'un stockage dans et en-dehors du Cloud… Il vaut mieux le faire à résilience, durabilité et performance égales.

4. Les moyens des fournisseurs de Cloud seront toujours (grandement) supérieurs aux vôtres

Notons tout d'abord qu'utiliser le Cloud, c'est un moyen efficace de confier ses activités de sécurité et de maintien en condition opérationnelle (MCO) des infrastructures à des experts dont c'est le cœur de métier.

On entend trop souvent que les Data Centers On Premise sont bien sécurisés : mais la réalité c'est que nous ne connaissons presque aucun Data Center qui chiffre l'intégralité de ses données, contrairement à ce qui se passe chez les Cloud Providers.

À titre d'illustration, un des plus gros hyperscalers emploie plus de 750 spécialistes Sécurité à plein temps. Les organisations ne pourront jamais en dire autant. Force est de constater qu'il existe un lien entre les moyens consentis et les résultats obtenus.

Un fournisseur de Cloud héberge vos données dans une région que vous aurez choisie. Les données ne sont déplacées dans une autre région que sur une initiative du client, et non du Cloud Provider. Enfin, si le lieu exact de l'hébergement n'est pas fourni, c'est dans le but de protéger l'accès physique aux données.

5. Se poser les bonnes questions

L’une des limites des offres Cloud en matière de sécurité porte sur leur date de « péremption » des offres. Dans le cas de la restauration de vos données, si vous voulez remonter au-delà de cinq ans, il faut se poser les bonnes questions et trouver des réponses adaptées en cas de disparition d’un service.

L’engagement des fournisseurs sur la durée de vie reste limité. Cela ne concerne pas tous les secteurs, ni toutes les entreprises, ni même tous les projets, mais c’est un point de vigilance.

Ce que fournit un Cloud Provider par défaut :

Systèmes de contrôle d’accès

Surveillance continue des menaces

Chiffrement des données en transit et au repos

Sécurité physique du Data Center

Protection du réseau

Sécurité des applications

Redondance des données

Validation continue

Protection contre la suppression massive de fichiers

Connexion suspecte et surveillance de l’activité

Pour conclure

Le Cloud offre une sécurité renforcée grâce aux investissements des fournisseurs dans des mesures de protection avancées et une gestion proactive des menaces. En termes de résilience, sa répartition géographique et les SLA garantissent la disponibilité continue des données et applications.

Le Cloud est donc un atout majeur pour améliorer la sécurité et la résilience des opérations informatiques, en s'entourant toujours de professionnels des services cloud pour maximiser ses avantages.

Le marché "Prestations réalisées en environnement cloud" de l'UGAP

Dans le sillage de la stratégie 'Cloud au centre' de l'Etat, l'UGAP propose à ses bénéficiaires de la sphère publique un marché qui leur permet d'accéder à l'ensemble des services nécessaires à leur transformation numérique vers le cloud. Atos et Open sont les titulaires de ce marché au cœur des politiques publiques.

Solution sélectionnée par UGAP Atos | Open

Pour en savoir plus

À propos d'Atos

Atos est un leader international de la transformation digitale avec 105 000 collaborateurs et un chiffre d'affaires annuel d'environ 11 milliards d'euros. Numéro un européen du cloud, de la cybersécurité et des supercalculateurs, le Groupe fournit des solutions intégrées pour tous les secteurs, dans 69 pays. Pionnier des services et produits de décarbonation, Atos s'engage à fournir des solutions numériques sécurisées et décarbonées à ses clients. Atos est une SE (Société Européenne) cotée sur Euronext Paris.

La raison d'être d'Atos est de contribuer à façonner l'espace informationnel. Avec ses compétences et ses services, le Groupe supporte le développement de la connaissance,de l'éducation et de la recherche dans une approche pluriculturelle et contribue au développement de l'excellence scientifique et technologique. Partout dans le monde, Atos permet à ses clients et à ses collaborateurs, et plus généralement au plus grand nombre, de vivre, travailler et progresser durablement et en toute confiance dans l'espace informationnel.

Plus d'informations sur nous

atos.net
atos.net/career

Entamons une discussion ensemble

À propos de Tech Foundations

Tech Foundations est la ligne de métier du groupe Atos leader dans les services d'infogérance, centrée sur l'infrastructure et le cloud hybride, l'expérience employé et les services technologiques, grâce à des solutions décarbonées, automatisées et tirant parti de l'IA. Ses 52 000 collaborateurs font progresser ce qui compte pour l'avenir des entreprises, des institutions et des communautés du monde entier. Tech Foundations est présent dans 69 pays et a réalisé un chiffre d'affaires de 6 milliards d'euros en 2022.

À propos d'Open

Avec 4 000 collaborateurs et un chiffre d'affaires de 400 M€ en 2022, Open se positionne comme le partenaire de confiance des grandes entreprises françaises publiques et privées, engagé dans leur transformation IT et digitale. L'entreprise intervient principalement en France et à l'international au Luxembourg et Roumanie. Sa mission : conseiller ses clients dans leur trajectoire de transformation, concevoir, réaliser et opérer des systèmes d'information agiles, résilients et sécurisés et apporter des solutions logicielles innovantes en mode Saas, en s'appuyant sur ses trois expertises : technologiques, industrielles et sectorielles.

Open inscrit sa raison d'être dans une logique d'avenir « Faire du numérique le vecteur de transformation d'un monde plus humain et durable"» en cohérence avec ses valeurs d'entreprise : Agilité, Responsabilité, Engagement.

Pour en savoir plus sur Open : www.open.global

103458 - WP security in the cloud (FR) - IT + AI