LA SOUVERAINETÉ NUMÉRIQUE EUROPÉENNE : sécurité, confidentialité et performance

Luc d'Urso, PDG du groupe Atempo.Wooxo, nous parle des actions menées par son entreprise pour bâtir la souveraineté numérique européenne tout en garantissant la sécurité, la confidentialité et la performance.

Luc d'Urso

Bio express
Entrepreneur depuis près de 30 ans, Luc d'Urso a débuté dans l'industrie du sport avec le développement des marques de planche à voile et snowboards Mistral et des skis nautiques et wakeboards Reflex, avant de co-fonder en 1997, l'opérateur de télécom Futur Telecom (MVNO). En 2010, il fonde Wooxo, un éditeur français de solutions logicielles dédiées à la protection et à l'exploitation sécurisée des données. La croissance organique combinée à des rachats ont permis la constitution du groupe actuellement composé de trois entités : Wooxo, Atempo et Nextino.

Atempo.Wooxo œuvre pour préserver l'écosystème des données. Dites-nous en plus sur votre cœur de métier.
Notre raison d'être émane d'une vision : la donnée est la ressource la plus précieuse du XXIe siècle et son exploitation est source de création de valeur. Cet actif stratégique est stocké et traité au sein de systèmes composés d'applications et de matériel toujours plus sophistiqués, plus complexes et plus hétérogènes. Nous voyons cet ensemble en perpétuelle mutation comme un écosystème, concept qui nous paraît plus approprié que celui d'environnement, généralement utilisé en informatique. À l'instar des écosystèmes naturels, la qualité d'un écosystème de données se mesure à sa capacité à évoluer dans le temps, à maintenir son équilibre, et à se rétablir rapidement en cas d'agression.
Notre métier consiste à préserver cet écosystème de tout sinistre : depuis des erreurs humaines de manipulation jusqu'aux catastrophes naturelles, en passant par les pannes matérielles, et depuis quelques années, les cyberattaques toujours plus nombreuses et dévastatrices. Plus particulièrement, notre intervention consiste à sauvegarder, à archiver et à déplacer les données de nos clients, au moyen d'un portefeuille de solutions :

- Miria : pour sauvegarder, synchroniser, migrer et déplacer les grands volumes de données et les fichiers non structurés entre stockages hétérogènes ;
- Lina : une solution de sauvegarde en continu des postes de travail fixes ou en itinérance ;
- Tina : pour la sauvegarde, la restauration et la reprise d'activité des serveurs physiques et virtuels.

En effet, une sauvegarde correspond à une copie des données qui peut être utilisée pour restaurer les données originales dans le cas où ces dernières seraient endommagées ou perdues (suppressions accidentelles, corruptions de fichiers, problèmes techniques…). Cela concerne généralement les données qui sont régulièrement utilisées au sein de l'organisation. Quant à l'archivage, il correspond à un ou plusieurs enregistrements de données, dédiés à une conservation plus ou moins longue dans l'éventualité d'une exploitation ultérieure.
Notre rôle, en tant qu'expert de la data protection, consiste avant tout à protéger l'écosystème de données de nos clients contre des cybermenaces, de plus en plus complexes et capables de contrer les systèmes de protection traditionnels. Le rempart ultime consiste à conserver une copie des données sauvegardées sur un média non connecté au système d'information (Air Gap). Afin de restaurer le maximum de données, nous mettons en place des dispositifs étroitement liés aux workflows et à la chaîne d'information de nos clients. Dans un hôpital par exemple, la priorité sera accordée au rétablissement du service d'urgence avant de passer aux applications qui sont moins indispensables.
D'autre part, notre expertise dans le data management nous permet d'offrir à nos clients de la visibilité sur le volume, les stockages, la typologie et les modifications enregistrées par leurs données.

Quels sont les principaux enjeux liés à la protection et à la migration de très grands volumes de données ?
La première difficulté réside dans l'obligation de garantir la disponibilité des données au sein de très gros volumes, notamment en cas de sinistre.

Nos clients ont besoin de ces informations vitales afin d'assurer leurs activités (sciences de la vie et de la terre, modélisation industrielle, véhicules connectés, industrie pétrolière, recherche génomique, média...). Nous ne pouvons donc en aucun cas interrompre leurs cycles de production parce que les données ne sont pas accessibles. De même, garantir l'accès à ces données requiert de les sauvegarder ou de les archiver de manière très rapide. Nous nous appuyons sur des algorithmes de traitement spécialement développés à cet effet, afin de faire face à cette exigence de vélocité qui ne cesse de croître. Au-delà, nous devons assurer la bonne répartition de ces données entre les différents types de serveurs. Les données « chaudes » dont nos clients ont besoin au quotidien, doivent être stockées dans des serveurs très performants et qui en conséquence, coûtent chers. Quant aux informations moins sollicitées, elles peuvent être sauvegardées dans des serveurs plus économiques. En parallèle, puisque ces données doivent être accessibles, nous devons les organiser de manière à en faciliter le tri. En cas de recherche, le client doit être capable d'identifier la typologie et de reconnaître l'usage de ces données le plus vite possible. Dans la post production cinématographique par exemple, notre rôle consiste à conserver leurs œuvres (les masters) afin de les mettre à disposition des différents intervenants qui assurent leur traitement (correction des couleurs, effets spéciaux, sous-titrage...) et ce, en temps réel. C'est ainsi qu'approximativement un film ou dessin animés sur deux produits aux États-Unis est traité par nos solutions. Il en est de même dans les jeux vidéos.
Miria est également utilisée dans des cas d'usage tels que la migration depuis un ancien serveur vers un nouveau, ou depuis un serveur sur site vers le cloud ou l'inverse, tout ceci sans perte de données et sans aucune interruption d'activité.

Avec le déploiement massif du télétravail, la protection des données est devenue une nécessité stratégique. Comment accompagnez-vous vos clients à ce niveau ?
Le passage au télétravail a significativement accru la surface d'exposition au risque cybercriminel. L'utilisation d'ordinateurs familiaux non contrôlés par les DSI et avec des antivirus et antimalwares non professionnels et rarement à jour, l'usage combiné pro-perso et la connexion au système d'information depuis un accès internet grand public non sécurisé constituent autant de failles de sécurité dans lesquelles les cybercriminels se sont engouffrés. Les cyberattaques ont ainsi redoublé en intensité et en sophistication depuis le début de la crise sanitaire. Afin d'y faire face, nous avons rejoint Open Solidarity, une initiative d'OVHcloud répondant à l'appel lancé par Cédric O, le Secrétaire d'État au numérique, pour aider à sécuriser les postes des utilisateurs en télétravail. Toute organisation professionnelle, sans distinction de sa localisation géographique dans le monde, a pu ainsi sauvegarder leurs données à l'aide de notre solution de sauvegarde Lina et les héberger gratuitement chez OVHcloud pendant toute la période de confinement. Dans la continuité de cette démarche et puisque le télétravail prend une proportion plus importante au sein des organisations, nous avons conçu des solutions destinées aux entreprises de toutes tailles (TPE, PME et ETI). Elles peuvent ainsi stocker leurs données sur leurs propres serveurs, en mode Cloud privé ou public auprès de nos prestataires d'hébergement souverains (OVHCloud, Outscale, Scaleway, Jaguar Networks, ASP Serveur...). Nos services sont conformes au RGPD ce qui représente un gage de sécurité et de confidentialité pour nos clients. Ils sont aussi à l'abri du Patriot Act américain. Notre rôle dépasse donc le simple service de sauvegarde pour satisfaire les obligations légales de nos clients et les protéger des risques juridiques et financiers liés.

Comment voyez-vous votre secteur évoluer dans les prochaines années ?
Au-delà de la croissance du volume de données qui est de l'ordre de 68 % par an, les données personnelles, qui constituent aujourd'hui la majorité de ce stock, vont devenir minoritaires. En effet, cette proportion sera remplacée par des données industrielles qui proviendront en grande partie de l'IoT ainsi que des applications métiers qui sont en train de se développer. Ce nouveau gisement sera donc massif puisque nous estimons qu'il y aura plus de 21 milliards d'objets communicants dans les prochaines années. En parallèle, l'hébergement dans le Cloud passera de 80 % à seulement 20 % d'ici dix ans. Ces données seront hébergées dans des serveurs de proximité, d'où l'émergence du Edge Computing. Il s'agit d'une vraie révolution parce qu'elle concerne non seulement le mode de stockage mais aussi la provenance des données.

Vous vous êtes récemment associés à OVHcloud et IBM afin de proposer aux organisations européennes une nouvelle solution de stockage. Dites-nous en plus.
Pour répondre aux besoins de sécurité, de souveraineté et de résilience des sociétés et des institutions européennes en matière de conservation des données, nous avons collaboré avec OVHcloud et IBM afin de mettre en place une offre de « Stockage-as-a-service ». Cette solution reposera sur le stockage sur bandes magnétiques conçues par IBM, sera orchestrée par notre plateforme logicielle Miria et optimisée par la technologie d'erasure coding d'OVHcloud. L'expertise combinée de ces trois acteurs permettra aux utilisateurs de disposer d'une solution unique répondant aux exigences réglementaires en matière de conservation de données tout en étant ultra-compétitive, et avec le meilleur rapport prix/performance. Ce projet est une vraie source de fierté française et européenne.

EN BREF

- *Une équipe de 200 collaborateurs*
- *Plus de 20 millions d'euros de chiffre d'affaires*
- *Présence dans 194 pays à travers le monde*
- *Les filiales du Groupe sont établies en Europe, aux États-Unis, en Chine, en Corée, et à Singapour*
- *Six implantations en France : Massy, Vannes, Toulouse, Marseille, Lyon et un laboratoire de recherche en Intelligence Artificielle à Orléans (Nextino)*