4 critères pour évaluer les applications de demain

Sommes-nous devenus dépendants du numérique ? Ce n'est pas vraiment un scoop : nombre d'entre nous font désormais des achats, effectuent des opérations bancaires, travaillent et communiquent même avec leurs amis et leur famille grâce au numérique, sans se déplacer.

Est-ce être dépendant ou plus libre ? Ce qui est sûr, en revanche, c'est que le mouvement s'accélère. La crise sanitaire, en particulier, a fait plus qu'augmenter notre recours à ces services numériques — il a également accéléré la numérisation de ce qui était auparavant encore majoritairement des expériences physiques.

Qu'il s'agisse de la consultation d'un médecin, de la visite d'une nouvelle maison ou du travail dans un atelier de fabrication, toutes ces expériences nécessitaient autrefois une présence physique et deviennent de plus en plus et irréversiblement numériques.

Satya Nadella, PDG de Microsoft, a déclaré en avril de l'année dernière que le monde avait vécu deux ans de transformation numérique en deux mois. Il s'est écoulé tout juste une année depuis, et le rythme de la numérisation n'a fait qu'augmenter.

Et quel est le point commun de toutes ces expériences numériques ? Elles sont fournies par le biais d'applications.

Les applications sont devenues le vecteur premier, et le plus visible, de l'expérience numérique. C'est la première, et souvent la seule, chose que voit un client. Alors, autant les soigner !

Et c'est là que cette évolution pose de vrais problèmes aux entreprises, qui ont parfois du mal à suivre le rythme. Car la fourniture et la sécurisation des applications impliquent de naviguer à travers une combinaison de réseaux locaux et étendus, de clouds publics ou privés, de CDN (réseaux de distribution de contenu) et d'autres infrastructures situées à la périphérie.

Aujourd'hui, la plupart des entreprises assemblent manuellement la logique applicative et les technologies de diffusion et de sécurité dans ces environnements, application par application, brique par brique, souvent sans disposer d'une vision globale du produit fini.
Cette approche crée hélas de nouvelles surfaces d'attaque, ouvre la porte à de nouvelles menaces et engendre en prime une incroyable complexité opérationnelle — source de coût accru.

Les solutions de périphérie de première génération (que nous appellerons « Edge 1.0 » par simplicité) étaient surtout des CDN conçus pour améliorer la diffusion de contenus lourds (souvent vidéo) avec une faible latence, afin qu'ils puissent être mis en cache physiquement au plus près de l'utilisateur final.

En évoluant, ces CDN (appelons-les désormais « Edge 1.5 »), ont ensuite ajouté des capacités de calcul en périphérie pour héberger des contenus plus dynamiques, ont même été « SaaS-ifiés » et on leur a ajouté une sécurité « suffisante » (oui, les guillemets ont leur importance !).
Mais ces offres Edge 1.0 et Edge 1.5 demeurent des solutions périphériques fermées, dont la

capacité est limitée à celle de leur propre infrastructure physique. Et elles créent finalement un nœud ou un saut supplémentaire dans la voie de livraison des applications.

Cela oblige entre autres les entreprises à adapter leurs applications à chaque fournisseur de solutions périphériques.

Mais ce n'est pas le pire : en fait, ces CDN sont avant tout conçus pour diffuser du contenu (souvenez-vous : les vidéos !). Et même si leur évolution « 1.5 » a permis de mieux prendre en charge le modèle SaaS et le dynamisme applicatif, ils ne répondent pas entièrement aux besoins des applications complexes les plus dynamiques, ils ne font pas de l'efficacité de la sécurité une priorité absolue et n'ont pas été conçus pour simplifier la gestion et les opérations dans un paysage multicloud hétérogène.

Bref, ils ne sont plus adaptés aux réalités des applications modernes et leur paysage opérationnel.

Quels sont les besoins en la matière ? Avant tout de pouvoir exécuter des containers applicatifs standards n'importe où, dans n'importe quel cloud public, privé comme dans le centre de données de l'entreprise. Le container est le plus petit dénominateur standard commun, et à l'intérieur est hébergée toute l'intelligence et toutes les spécificités de l'application — mais lui-même demeure parfaitement standard.

Et ce container doit pouvoir être déplacé, déployé, fourni selon les modes opératoires choisis par l'entreprise, sans préférence. Et le tout doit pouvoir bénéficier des dernières avancées en matière de sécurité (dont le filtrage applicatif, la protection contre le bourrage d'identifiants, etc.), de manière là aussi standard.

Cela pourrait être le « Edge 2.0 », qui perpétue la tradition tout en s'adaptant au monde actuel, dont l'une des particularités est un fort niveau d'hybridation entre infrastructures on-premise, modèle SaaS, et Cloud public et privé, en mode PaaS notamment pour la construction des applications.

En particulier, l'un des aspects les plus passionnants de Edge 2.0 est la manière dont il fera progresser la notion d'applications « adaptatives ». Des applications qui s'adaptent naturellement à leur environnement — en grandissant, en se réduisant, en se défendant et en se soignant — afin que les entreprises puissent se concentrer sur leur cœur de métier.

L'approche Edge 2.0 permettra d'atteindre ces objectifs grâce à plusieurs fonctions importantes :

– **Automatiser les processus redondants** : Edge 2.0 doit s'appuyer sur une plateforme universelle de livraison d'applications. « Construire une fois, déployer globalement » doit devenir le leitmotiv des développeurs et des opérations. Cela permettra d'automatiser la distribution des applications à travers le centre de données, le cloud et la périphérie sans distinction et sans refaire le travail. Cela signifie donc la fin de l'intégration manuelle et fastidieuse des applications traditionnelles dans les environnements multicloud.

– **Offrir une sécurité de premier plan et de bout en bout** : qu'il s'agisse de protéger les applications elles-mêmes contre l'usurpation des identités et l'exploitation de vulnérabilités ou plus globalement de lutter contre la fraude, il est vital que chaque déploiement, chaque application, puisse avoir accès aux meilleures technologies de sécurité, où qu'elle se trouve (y compris à la

périphérie), en mode SaaS.

– **Augmenter l'agilité applicative** : à l'aide de conteneurs et d'API standard, les applications peuvent être mises sur le marché et s'adapter aux conditions changeantes beaucoup plus rapidement et de façon transparente, par rapport aux modèles de développement et de déploiement traditionnels

– **Capitaliser sur la connaissance des applications** : avec Edge 2.0, il est possible d'avoir une vue de bout en bout des performances et de la sécurité des applications. Et c'est justement cette précieuse télémétrie qui permettra en définitive de rendre les applications plus intelligentes, plus perspicaces et surtout plus adaptables (grâce à des règles qui permettront d'adapter le niveau de sécurité, la puissance de l'hébergement ou agir sur d'autres paramètres en fonction des informations remontées par l'application)

En fin de compte, le passage du modèle « Edge 1.5 » à « Edge 2.0 » est bien plus que la simple incrémentation que ne le suggère le nom : c'est une redéfinition de la manière dont les applications sont déployées et interagissent, afin de les rendre capables de répondre aux enjeux naissants d'un monde ou l'application devient le centre de l'interaction entre l'entreprise et ses (futurs) clients !