

Prévisions pour 2020 : Perspectives pour le cloud, les médicaments et les véhicules connectés, et la cybersécurité

17 décembre 2019

Peter Galvin | Directeur de la stratégie

[En savoir plus sur ce contributeur >](#)

Véhicules autonomes. Informatique dématérialisée. Médicaments connectés. Fuite de données.

Ces innovations, ces utilisations et ces défis sont au cœur des débats techniques depuis plusieurs années. Et les éléments mentionnés ci-dessus sont voués à connaître de profonds changements dans les années à venir.

Ces évolutions potentielles seront le fruit d'un ensemble de découvertes, d'avancées technologiques et d'amélioration organisationnelle récentes. Et la plupart apporteront des changements positifs.

Alors, à quoi pouvons-nous nous attendre dans ces domaines importants en 2020 ? Je vous présente ici mes prévisions.

Le chemin à parcourir pour la voiture autonome se fait de plus en plus long et étroit

Vous n'êtes pas les seuls à penser que les véhicules qui se conduisent eux-mêmes relèvent de la science-fiction. Beaucoup d'entre nous croient que l'on est bien loin de voir les voitures autonomes être utilisées un peu partout. Et c'est effectivement le cas.

Comme chacun sait, les véhicules autonomes existent aujourd'hui dans notre monde. Cependant, cela ne veut pas dire que nous les verrons rouler de sitôt sur les Champs-Élysées. Au contraire, la majorité des véhicules autonomes qui seront prochainement commercialisés auront un rayon d'action limité et ne seront utilisés que sur de courtes distances.

En soi, trouver le moyen de mettre en circulation des véhicules autonomes sans problèmes est un énorme défi. Il est donc compréhensible que de tels essais puissent se heurter à certaines embûches. Toutefois, les véhicules autonomes se heurtent à des problèmes beaucoup plus graves que prévu, notamment [une collision mortelle](#).

C'est pourquoi les véhicules autonomes sont une technologie nettement plus éloignée de nous que ce qui avait pu être prévu au début. C'est pour cela que nous allons assister à un changement dans la façon dont ils seront utilisés. Ils seront limités à certains itinéraires, à certaines vitesses et utilisés uniquement pour couvrir certaines distances. Comme pour une navette de ski, ils suivront une piste bien spécifique et n'auront qu'un petit nombre de tâches à accomplir.

L'effet boomerang stimule l'adoption du multi-cloud et du multi-déploiement

IDC estime que les [dépenses consacrées aux services de cloud public à travers le monde](#) s'élèvent à 190 milliards d'euros cette année et devraient atteindre près de 420 milliards d'euros d'ici 2023. Et une étude réalisée par Gartner révèle que [81 % des utilisateurs de cloud public utilisent deux ou plusieurs fournisseurs](#). Mais Gartner déconseille aux entreprises de passer immédiatement de la gestion sur site au multcloud. Les différences entre les plates-formes compliquent en effet la mise en place de services sur plusieurs d'entre elles. Par conséquent, les entreprises devraient plutôt donner à leur personnel le temps de se former au cloud.



Malgré ces difficultés, je suis convaincu que le multcloud sera de plus en plus adopté au cours des prochaines années. Mais je crois aussi que, parallèlement aux cloud publics, 2020 sera une année où l'on mettra davantage l'accent sur les technologies destinées aux environnements privés sur site et sur cloud. On peut imputer cela à l'effet boomerang.

Il y a tout juste deux ans, de nombreuses organisations prévoyaient de passer à 100% au cloud public. Et, dans certains cas, ces entreprises ont déplacé un certain nombre de leurs applications vers le cloud. Pendant ce processus, beaucoup d'entre elles ont découvert que le cloud public ne répondait pas forcément à tous leurs besoins. Cette prise de conscience a notamment été provoquée par les problèmes de sécurité et la nécessité de modifier les applications, parmi d'autres défis imprévus. C'est ainsi que certaines applications sont revenues aux déploiements sur site.

De nos jours, les organisations adoptent de plus en plus des environnements multi-cloud et multi-déploiement. Ils déploient des applications parce que celles-ci reposent sur les meilleures technologies et parce qu'elles sont sécurisées, peu importe qu'elles soient sur site ou sur cloud.

Je pense que nous continuerons à voir se développer des applications commerciales qui imitent les environnements cloud, même si, techniquement, elles ne relèvent pas du cloud public. Les organisations développeront leur infrastructure et leur architecture de manière à pouvoir étoffer et enrichir les applications, en plus de pouvoir gérer les charges de travail. Ces environnements ressembleront fortement aux clouds publics, sauf qu'ils seront conçus sur site ou au sein de clouds privés.

Les médicaments connectés multiplient les visites à domicile

Il y a quelques années, WIRED a publié un article intitulé «[Healthcare 2020: The e-Doctor Will See You Now](#). » Cet article faisait état de la diminution probable des procédures papier dans la profession médicale. Il indiquait que les patients auraient progressivement un plus grand

contrôle sur leurs soins de santé. Il précisait en outre que des dispositifs portables permettraient de suivre la santé des patients où qu'ils se trouvent.

Dans une certaine mesure, ces tendances se dessinent déjà. Il faut s'attendre à ce qu'elles prennent encore plus d'ampleur au cours des prochaines années.

En 2020, de grands appareils médicaux comme les respirateurs feront leur apparition dans les foyers alors qu'ils n'étaient auparavant disponibles qu'au sein des établissements médicaux. Ces appareils seront plus petits, connectés à Internet et pourront être utilisés à domicile car ils fonctionnent en réseau. La possibilité de disposer de ces machines à domicile optimisera les processus de soins. Elles amélioreront la santé et sauveront des vies.

Les fuites de données demeurent un défi de premier plan

La multiplication des appareils connectés et la transmission de données personnelles vers des systèmes connectés accroissent les risques. C'est pourquoi en 2020, il y aura autant, sinon plus, de fuites de données qu'en 2019.

Les fuites de données sont autant de vaches à lait potentielles pour les cybercriminels. Les hackers solitaires sont devenus des groupes criminels organisés qui traquent les [données à caractère personnel](#).

Et les données médicales constituent un véritable trésor de données pour les malfaiteurs. Certaines études indiquent que [les dossiers médicaux complets peuvent rapporter jusqu'à 850 € sur le dark web](#). Il s'agit là de bien plus que de simples données de carte bancaire ou de numéro de sécurité sociale. Des personnes non autorisées pourraient accéder à des dossiers médicaux [en piratant des dispositifs portables et implantés](#) et ainsi se retrouver au cœur d'un système de santé avec les dossiers médicaux électroniques des patients.

Bien d'autres éléments viennent également fragiliser la situation. Il s'agit notamment des erreurs humaines et des entreprises qui peinent à trouver le bon équilibre entre « juste assez » et « trop » de sécurité.

Les organisations doivent mettre en place des systèmes de sécurité et de protection de la confidentialité, à condition que ces mesures ne soient pas trop nombreuses pour éviter de faire fuir les consommateurs. Tout le défi consiste à trouver le point d'équilibre idéal. Les organisations pour lesquelles la sécurité est insuffisante se retrouveront forcément confrontées à des fuites de données au cours des prochaines années.

Rendez-vous sur notre [site web](#) pour découvrir nos solutions de sécurité. Vous pouvez également nous suivre sur [Twitter](#), [LinkedIn](#), et [Facebook](#).