

## **Préparez les Entreprises à l'Arrivée des Wearables Connectés**

### **Info**

Posté par : JulieM

Publié le : 21/11/2013 11:30:00

Quel que soit l'endroit où l'on regarde ces derniers temps, il semblerait que les montres connectées, ou plus précisément les wearable technologies, soient sur le point de devenir la dernière grande mode en matière de technologie. Samsung a sa Galaxy Gear, Sony sa Smartwatch et même le fabricant automobile Nissan suit le mouvement avec Nismo, sa propre montre intelligente connectée.

Même si Google avec ses Google Glass est manifestement l'un des plus gros acteurs sur le marché de l'informatique vestimentaire, Apple, LG et bien d'autres encore ont tous montré leur intérêt pour ce nouveau marché. D'après la société américaine Gartner Inc., le marché mondial des wearable technologies pourrait valoir 7,4 milliards d'Euros d'ici 2016.

Il semblerait également que le futur des technologies vestimentaires soit très prometteur, en particulier pour les secteurs de l'industrie qui pourraient bénéficier d'un avantage évident grâce à l'utilisation de technologies gestuelles ou à la possibilité d'avoir accès à un appareil tout en ayant les mains libres. Les secteurs de l'industrie, de l'expertise et même la chirurgie n'en sont que trois exemples parmi tant d'autres. Ces technologies seraient mises en place au sein des entreprises de façon minutieuse ; elles auront certainement des coûts élevés, des budgets élevés et des déploiements de façon délicate.

Le plus gros problème est alors de savoir comment les entreprises vont-elles pouvoir gérer les gadgets vestimentaires conçus pour les consommateurs ? En effet, si ces objets deviennent aussi communs que les Smartphones aujourd'hui, l'impact sur les réseaux informatiques des entreprises sera considérable.

Pour commencer, prenons l'exemple des Smartwatch, qui doivent être associées à un Smartphone (ou un appareil similaire). Ce nouveau type de montres accessoirise les téléphones, tablettes et ordinateurs portables mais en aucun cas ne les remplace. Les accessoires intelligents connectés comme les lunettes, les chaussures, les bijoux et bien d'autres encore vont de ce fait venir multiplier le nombre d'appareils permettant un accès à un réseau. Pour tous ceux qui voyaient l'arrivée du BYOD comme un véritable challenge, attendez-vous à devoir le multiplier par cent avec la révolution des wearables et accessoires connectés.

Les lunettes 'Google Glass' pourront enregistrer tout ce que voit la personne qui les porte. De la même manière, les montres connectées auront également des fonctions d'enregistrement et de camera. Au premier abord, ces gadgets peuvent donner l'impression de sortir tout droit d'un film d'espionnage, pourtant, transférer en toute discrétion, des informations sensibles et secrètes vers un appareil se trouvant en dehors du réseau de l'entreprise pourrait devenir un véritable jeu d'enfant.

La bonne nouvelle pour les réseaux des entreprises, c'est que le fait de se préparer à cette révolution permettra de réduire, de manière considérable, les perturbations les plus redoutables. En effet, les entreprises qui gèrent déjà, de manière efficace, les problèmes engendrés par le BYOD en termes de politiques, de sécurité, de gestion et de contrôle réseau, auront déjà un réel avantage pour faire face à cette révolution.

Dans le cas où les entreprises souhaiteraient adopter les technologies vestimentaires ; et beaucoup s'accordent à dire que ce n'est qu'une question de temps avant qu'elles n'y soient obligées, il faudra mettre en place des politiques claires qui déterminent qui est autorisé à

apporter un tel appareil au sein de l'entreprise et à le connecter au réseau.

Sur les réseaux informatiques, les vêtements et accessoires connectés vont avoir un impact sur deux choses : l'accès et les paramètres de sécurité. Alors qu'aujourd'hui, les employés apportent au sein de leur entreprise entre un et trois appareils mobiles permettant un accès réseau, il se pourrait que dans quelques années, il y en ait 15 à 20 par employé.

Les entreprises doivent donc se préparer aux principaux modes d'accès, c'est-à-dire le Wi-Fi et le Bluetooth. Dans le cas où le Wi-Fi est utilisé, il faudra porter une attention toute particulière à ce que l'infrastructure puisse gérer une arrivée en masse de nouveaux appareils.

Du point de vue de la sécurité, les plus gros problèmes auxquels il faudra faire face seront la gestion des données qui circulent sur le réseau et la possibilité de les surveiller. Tout d'abord, il est tout à fait légitime de déterminer quel appareil a accès au réseau ou quelles sont les données qui y transitent. Ensuite, avec l'affluence d'appareils divers sollicitant une connexion, votre réseau sera plus vulnérable quant aux attaques malveillantes sous forme de virus ou autres menaces informatiques.

Enfin, le flux des données transitant sur les réseaux va devenir beaucoup plus complexe. En effet, alors que la plupart des gadgets pourront accéder au réseau via le Wi-Fi ou le Bluetooth, ils nécessiteront toujours une connexion à un ordinateur portable, de bureau ou à une tablette afin de pouvoir synchroniser les données, ce qui pourrait ralentir davantage le réseau.

Si la surveillance réseau et la détection des intrusions sont faites sur le moment et ne sont pas soutenues par une bonne infrastructure et des politiques faites sur mesure, les réseaux des entreprises en subiront les effets et connaîtront de gros ralentissements. Si elles veulent éviter les problèmes de capacité et de sécurité, les entreprises doivent prêter attention à ces scénarios et commencer à s'y préparer en avance.

Pour ce faire, elles peuvent adopter deux solutions : le 'scale out' ou le 'scale up'.

Choisir le 'scale out' signifie qu'elles vont devoir se préparer à l'arrivée en masse de nouveaux appareils en extrapolant le nombre de points d'accès et en assistant les systèmes de détection d'intrusion. Des investissements seront nécessaires, il faudra une surveillance réseau supplémentaire et il se pourrait que cela implique des problèmes en matière de capacité ou de ralentissement.

Choisir le 'scale up' signifie qu'elles devront améliorer leurs infrastructures afin de pouvoir gérer au mieux l'affluence prévue de nouveaux appareils. Les investissements requis sont conséquents mais cela signifie également que la capacité du réseau sera en mesure de faire face à la demande. Cependant, choisir cette option n'exclut pas une surveillance réseau supplémentaire. En effet, l'infrastructure devra prendre en charge un système de surveillance (via lequel les tablettes, ordinateurs portables, téléphones, etc. accèdent au système) plus tridimensionnel que celui actuel pour prendre en compte quels autres appareils ou informations peuvent se connecter les uns/unes aux autres.

Au final, que la technologie vestimentaire ait un impact sur la gestion réseau des entreprises cette année ou l'année prochaine et que vous choisissiez la solution 'scale up' ou 'scale out', la chose qu'il ne faut absolument pas négliger est de s'assurer que la gestion de ces nouveaux appareils tiendra compte d'une solide politique BYOD. Parce que comme vous le savez, avec la gestion réseau, garder une longueur d'avance vous évitera d'être pris au dépourvu. Par Ennio Carboni, directeur de la gestion réseau chez Ipswitch, Inc.

À