

5 clés d'une stratégie mobile performante



Smartphones, tablettes, PC ultra-mobiles ont libéré les utilisateurs et transformé les interactions entre les collaborateurs. Encore faut-il que l'entreprise leur procure une connectivité mobile fiable, performante et sécurisée à même de fluidifier ces nouveaux usages...

La mobilité est un usage autant qu'une nécessité. **Les smartphones, les tablettes, et les ultrabooks ont dissocié travail et bureau.** Au sein même de l'entreprise, les collaborateurs, mais aussi les clients et les partenaires, s'attendent à être connectés à la fois parce que les outils qu'ils utilisent sont de plus en plus souvent « en ligne » mais aussi parce qu'une bonne collaboration d'équipe implique une multiplication des interactions sous des formes les plus variées (visio, téléphonie, tchat, réseau social).

Aujourd'hui, six employés sur dix affirment que les technologies mobiles les rendent plus productifs, selon une étude menée par « The Economist Intelligence Unit ». **Si la mobilité est devenue un vecteur d'efficacité et de disponibilité, elle demeure aussi un challenge technique.** En effet, toute mobilité d'entreprise repose sur trois fondations techniques inébranlables qui doivent focaliser toutes les attentions : le réseau, la connectivité, et la sécurité.

Au-delà de la maîtrise technique - qui dépend en partie des équipements et en partie de la compétence des équipes de la DSI - il est essentiel d'aborder la mobilité comme un vrai projet d'entreprise avec une vision stratégique à long terme et une bonne compréhension à la fois des risques induits mais aussi des atouts qu'elle engendre en matière de confort de travail, de créativité, et de productivité. On estime, ainsi, que, **d'ici**

2020, l'entreprise devra accueillir **4,3 appareils connectés par personne présente dans ses murs**, un chiffre qui enflera avec la multiplication des capteurs IoT dont l'entreprise aura besoin dans la modernisation de son Business.

Voici les 5 clés essentielles d'une stratégie mobile performante...

1. Faire une étude de couverture

Les technologies sans-fil reposent sur les ondes radios. Mais ces dernières sont capricieuses. Elles constituent une science à part entière qui s'abreuve de difficultés techniques complexes dénommées interférences, réfractions, et autres diffractions. Au sein d'un bâtiment, les sources de perturbations des signaux sont nombreuses et les différentes cellules Wi-Fi sont, elles-mêmes, susceptibles de s'interférer entre elles si l'on n'y prend pas garde et si l'on n'y applique pas les réglages adéquats.

En outre, les ondes ne sont pas bornées aux murs de l'entreprise et s'en échappent soulevant des risques potentiels de sécurité qu'il faut savoir appréhender et limiter.

Identifier toutes les sources possibles d'interférences, ainsi que les risques de sécurité, réclame expertise, minutie et expérience. Mais cette étude de couverture est primordiale pour garantir la fiabilité de votre réseau, optimiser vos investissements et maîtriser les périmètres de sécurité.

2. Penser le réseau comme un tout

Pour aussi essentielle qu'elle soit, l'étude de couverture doit aussi s'accompagner d'une étude sur la capacité du réseau sans-fil et celle du réseau filaire auquel sont reliés les équipements Wi-Fi. D'autant que le Wi-Fi se fait sans cesse plus rapide et nécessite une bande passante de réseau fédératrice. Avec la généralisation de la norme 802.11ac et l'arrivée des normes 802.11ad et 802.11ax, les extrémités du réseau vont aussi nécessiter des tuyaux Internet plus importants pour gérer le trafic sans fil accru. **D'une manière générale, tous les équipements vont devoir suivre et satisfaire les pics éventuels.**

Par exemple, les nouveaux points d'accès Aruba Instant 802.11ac offrent des vitesses Wi-Fi Gigabit avec des performances 36% plus élevées que les solutions concurrentes lorsqu'un grand nombre d'appareils mobiles sont simultanément connectés et une excellente fiabilité avec aucun point unique de défaillance et des capacités de survie réseau jusqu'au dernier point d'accès.

Ces solutions sont évolutives et utilisent une même interface centralisée offrant une visibilité complète sur tout le réseau.

3. Investir dans une sécurité de bout en bout

La sécurité est un long chemin pavé d'embûches et non une destination. La multiplicité des appareils mobiles et l'arrivée de l'IoT (encore très immature en matière de sécurité) constituent des pièges majeurs. En outre, le Wi-Fi est sans doute la norme réseau qui évolue le plus fréquemment. Chaque évolution doit vous inviter à remettre en cause l'étude de couverture réalisée et à ajuster vos stratégies de sécurité.

Dès lors, la sécurité doit être pensée pour ces nouveaux défis. Elle doit s'étendre à l'intégralité du réseau, de façon uniforme, en s'appuyant sur des stratégies de sécurité simples à définir, à maintenir et à faire évoluer.

Des solutions comme Aruba ClearPass favorisent une telle approche à l'aide d'une gestion intégrée des stratégies de sécurité qui s'étend à toute l'entreprise, et notamment à ses composantes mobiles, que les connexions soient filaires, sans-fil ou via des VPNs. Elle procure à l'IT **une vue complète des utilisateurs (et leurs rôles et droits), des appareils connectés (y compris leur type, leur position géographique, et autres attributs)** et donne un contrôle complet sur « qui » a accès aux ressources internes mais aussi « quand » et « d'où ».

Cette solution logicielle vient en complément des sécurités embarquées au cœur même chaque point d'accès Wi-Fi (pare-feu PEF, protection contre les intrusions RFPProtect, etc.) pour amener la sécurité au plus proche de l'utilisateur. Chaque borne devient ainsi un élément proactif de la sécurité du réseau et de l'entreprise.

4. Se focaliser sur l'expérience utilisateur

L'expérience utilisateur est capitale et influe beaucoup sur la perception que l'utilisateur a de son entreprise. L'utilisateur doit pouvoir se déplacer sans systématiquement se reconnecter et

se réauthentifier.

Il doit être en mesure d'enrôler, par lui-même, ses terminaux dans le réseau et se voir appliquer les sécurités qui conviennent. Clients et partenaires doivent, aussi, pouvoir se connecter pour profiter d'Internet sans compromettre la sécurité grâce à des droits minimaux. Il faut aussi **veiller au fonctionnement fluide du réseau notamment à l'heure où les utilisateurs consomment de plus en plus de flux vidéos et utilisent leurs appareils mobiles comme des terminaux de communication universels** (Téléphonie, visioconférence, VoIP, messagerie instantanée, etc.).

Pour garantir une expérience fluide, vous devez mettre en place une solution de gestion réseau simple d'utilisation et flexible pouvant évoluer avec votre entreprise et préférer les équipements qui offrent un pilotage centralisé « on-premise » (tel Aruba AirWave) ou via le Cloud (à l'instar d'Aruba Central).

5. Capitaliser sur l'utilisateur connecté

Une connectivité Wi-Fi est un véritable atout pour la productivité, l'efficacité et le bien-être des collaborateurs à condition que l'expérience utilisateur soit soignée et que l'environnement de travail tire profit de cette mobilité.

Il faut capitaliser sur cette connectivité en adoptant des solutions de communication mobile unifiée telle Office 365 et en favorisant le travail collaboratif (Teams, Slack, ...) et le partage de l'information (Sharepoint, Yammer, ...).

Tous ces outils ne peuvent s'exprimer qu'avec une infrastructure mobile opérationnelle. **Il faut, également, repenser les applications métiers pour la mobilité et les terminaux qui l'accompagnent** (tablettes, smartphones, 2-en-1, etc.). Enfin, il faut réfléchir à tous les scénarios rendus possibles par cette connectivité mobile et savoir en tirer profit.

L'accompagnement avec un partenaire de confiance

Mieux vaut ne pas s'aventurer seul.

Une stratégie mobile performante nécessite expériences et compétences et ne laisse aucune place à l'improvisation et aux expériences tatillonnes. Pour mieux accompagner ses clients, Misco-inmac wstore a mis en place des pôles de compétences reconnus. Les domaines concernés vont de la mobilité à l'infrastructure en incluant l'architecture réseau, la sécurité, les communications unifiées et les solutions d'impression.

Son pôle Solutions & Expertises vous accompagne dans vos projets de transformation numérique.

De l'audit au déploiement de flottes mobiles, en passant par la gestion de parc, la réparation ou l'échange de terminaux, l'accompagnement de leurs experts va plus loin.

Que ce soit Windows 10, Office 365, Android ou encore iOS, des équipes dédiées vous conseillent sur tous les aspects de votre projet mobilité et cela, jusqu'aux solutions de déploiement et de distribution de contenus.

Les Experts Mobilité travaillent en étroite collaboration avec les Experts Réseaux (certifiés partenaire Gold HPE Aruba Networks) pour faire bénéficier aux entreprises d'un accompagnement global, du projet mobilité jusqu'à la mise à niveau de votre réseau filaire et wifi.

