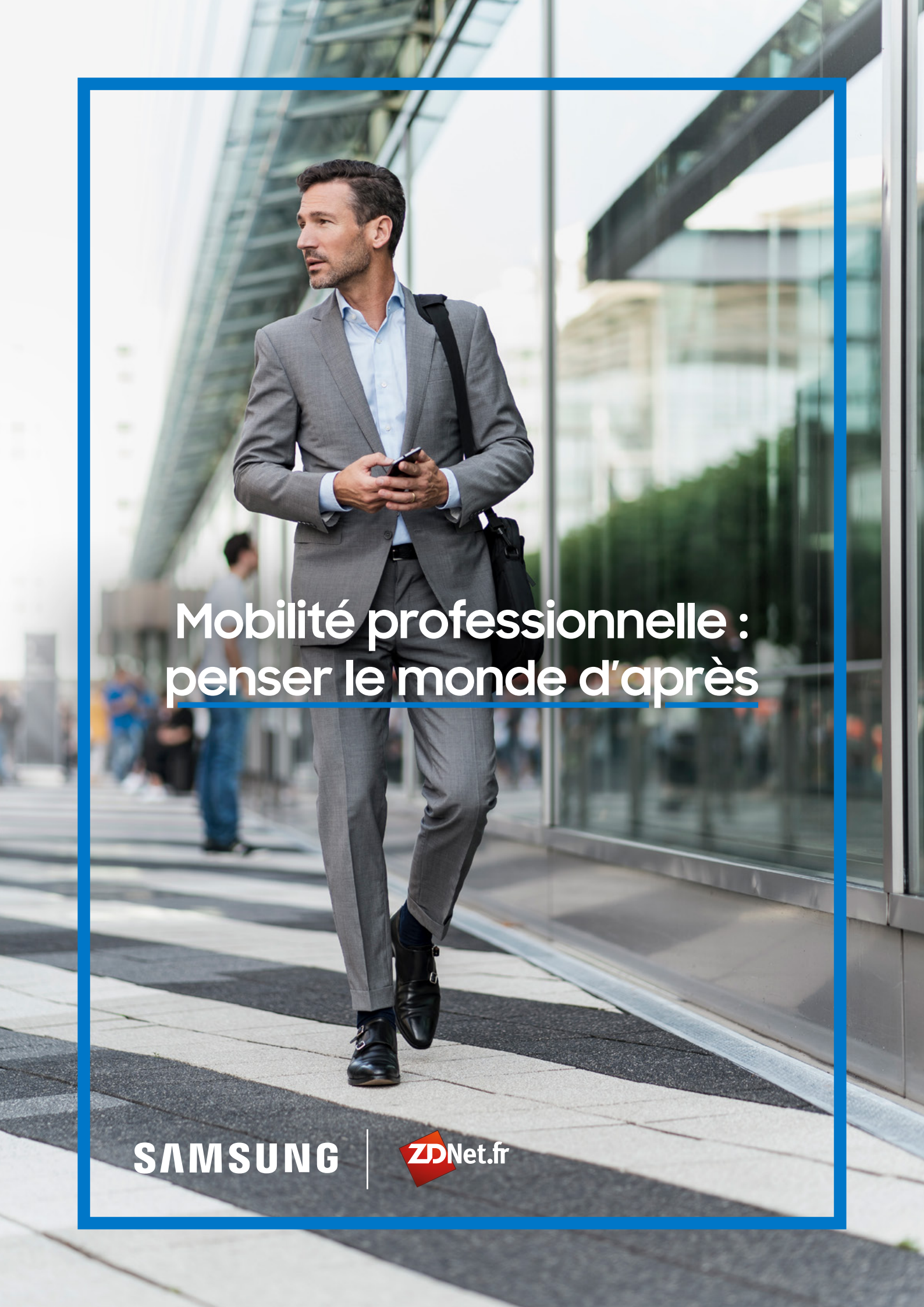

Mobilité professionnelle :
penser le monde d'après
SAMSUNG
ZDNet.fr

En mars 2020, le monde a vu ses habitudes transformées par une crise sanitaire de grande ampleur. En France, le confinement qui en a découlé a bouleversé de nombreuses entreprises et les a incités à repenser leurs modes de travail et d'organisation.

Bien que la mobilité se soit beaucoup développée ces 5 dernières années, cette période de confinement a accéléré le déploiement de nouvelles méthodes et outils de travail numérique : télétravail à 100%, horaires aménagées, explosion des réunions à distance, nécessité de sécurisation poussée des outils mobiles, usages quotidiens de nouvelles technologies et applications...

La mobilité professionnelle est à un tournant et n'a jamais progressé aussi vite. Cela ne va pas s'arrêter.

Samsung s'est associé à ZDNet, le site d'information de référence des décideurs IT, afin de vous donner les clés de la mobilité professionnelle pour **" penser le monde d'après "**.

Bonne lecture.

SOMMAIRE

L'ACCÉLÉRATION DE LA TRANSFORMATION NUMÉRIQUE DES ENTREPRISES

MOBILE WORKPLACE : LE BUREAU RÉINVENTÉ SOUS LE SIGNE DE LA PRODUCTIVITÉ

LA SÉCURITÉ MOBILE, PLUS QUE JAMAIS AU CENTRE DES PRIORITÉS DES ENTREPRISES

L'ACCÉLÉRATION DE LA TRANSFORMATION NUMÉRIQUE DES ENTREPRISES

Une nouvelle organisation du monde du travail est en œuvre. Les mesures de confinement en France et à travers le monde ont obligé l'ensemble des acteurs à apprendre à travailler autrement. La tendance de la transformation digitale des entreprises est devenue instantanément une évidence : les sociétés doivent s'adapter à un nouveau monde où le travail ne se fera plus forcément en présentiel. Au cœur de cette mutation "forcée" : la mobilité et les outils digitaux. Cette crise a été un accélérateur de la transformation numérique de la société et des entreprises. Avec à la clé, un bouleversement général des modes de travail et d'interaction que nous vous proposons de décrypter.

COMMENT LA CRISE A ACCÉLÉRÉ LA TRANSFORMATION DIGITALE INTERNE ?

De nouveaux outils, comme la visioconférence, et des méthodes de travail plus collaboratives ont déboulé dans les entreprises durant la crise. Contraintes d'innover, elles ont fait progresser la transformation digitale interne. Son aboutissement n'est cependant pas acquis.

Le 17 mars, le confinement est entré en vigueur en France. Les entreprises ont été contraintes dans ce cadre d'organiser le travail à distance de leurs collaborateurs. Les mieux préparées ont eu besoin de quelques jours pour s'adapter à ces nouvelles conditions. Toutes les organisations n'étaient pas prêtes, technologiquement et culturellement, à basculer sur cette configuration.

Elles ont dû par conséquent opérer une transformation digitale interne dans des délais record, là où DSI et CDO avaient pu jusqu'à présent se heurter à des résistances. Pour le vice-président Digital Business Innovations chez PAC, Olivier Rafal, indéniablement, *"on n'innove jamais aussi bien que sous la contrainte."*

Une prise de conscience à l'égard du digital interne

La crise a joué le rôle *"de révélateur au sein des entreprises ayant investi dans des plateformes agiles de type cloud et outils collaboratifs. Elles ont rapidement pu mettre en place les procédures nécessaires, notamment de télétravail"* constate-t-il. Pour les autres sociétés, le passage à une ère du travail sous confinement s'est révélé plus délicat. Que ce soit dans leur culture ou leurs infrastructures informatiques, ces dernières n'ont pas bénéficié d'une agilité comparable, faute d'investissement. Les évolutions opérées en urgence ont cependant été sources d'enseignements.

"Des entreprises ont dû élaborer en catastrophe de nouvelles solutions et instaurer du télétravail généralisé. Et elles se rendent compte globalement que ces modes de travail fonctionnent plutôt bien. De nouvelles méthodes, voire des business models, pourraient donc émerger de cette période de crise" avance Olivier Rafal.

Pour le consultant d'Abalon, spécialiste du *"digital workplace"*, le Covid a clairement fait bouger les lignes sur le digital interne. Christophe Coupez parle même *"de claque"* pour ces entreprises où le sujet du télétravail était bien souvent considéré comme "tabou". *"Un DSI m'a expliqué avoir avancé plus en quelques jours sur le télétravail qu'en dix ans de palabres"* témoigne-t-il. Pour ces sociétés, il a cependant fallu avancer dans l'urgence sur les outils, *"déjà un sacré problème"*, mais aussi sur les approches du télétravail.

La visioconférence, grande gagnante de la crise

L'adoption de certaines solutions du marché comme Microsoft Teams ou Zoom dans le domaine de la visioconférence traduit cette adaptation soudaine. Nombre d'entreprises ont souscrit à des outils collaboratifs, d'accès à distance et de sécurité, confirme le cabinet PAC. Tous ne seront pas pérennisés ensuite.

Il y aura bien néanmoins un avant et un après.

> *"De nouvelles crises pourraient survenir. S'il était admissible lors du Covid de ne pas être préparé, ce ne le sera en revanche pas du tout à la prochaine crise. Il faut penser résilience de son système d'information, mais aussi mobilité et sécurité."*

L'abonnement à des logiciels cloud, en particulier pour la visioconférence, a explosé lors du confinement. Le directeur des infrastructures d'Engie le confirmait lors d'un webinaire début mai. Le nombre d'utilisateurs quotidiens a été multiplié par dix dans l'entreprise. Les chiffres des fournisseurs l'attestent.

Fin avril, Microsoft Teams comptait par exemple plus de 75 millions d'utilisateurs actifs par jour. Zoom dépassait quant à lui les 300 millions. L'usage de la visioconférence n'est pas néanmoins la preuve d'une transformation digitale réussie, met en garde Christophe Coupez. *"La transformation numérique, ce n'est pas uniquement déployer Teams, et surtout pour faire de la visioconférence. C'est beaucoup plus profond. Cela touche l'organisation, la culture managériale, les relations entre les équipes, etc. La crise a d'abord servi à démontrer l'importance de disposer d'un outil sur le cloud pour s'affranchir d'une infrastructure."*

Les outils ne font pas la transformation digitale

Le consultant d'Abalon constate en effet souvent que les usages restent circonscrits à certaines fonctionnalités seulement et peu soucieux de bonnes pratiques. L'application de Microsoft peut ainsi parfois être utilisée comme simple alternative à un serveur de fichiers. *"Le vrai indicateur permettant d'évaluer l'adoption de Teams, c'est la baisse drastique du nombre d'emails échangés en interne combinée à la hausse des publications sur Teams. Si vous n'avez qu'aucune augmentation des visios sans réduction de l'email, alors il n'y a pas de transformation"* insiste-t-il.

Christophe Coupez estime donc que la fin du confinement pourrait déboucher sur un retour aux anciennes pratiques digitales faute d'un accompagnement sur les usages ou du fait de mauvaises expériences. *"La crise du Covid a permis de comprendre qu'il fallait du cloud, mais pas le reste"* ajoute-t-il.

L'après confinement devrait donc être selon lui consacré à un travail de gouvernance afin de structurer l'utilisation des applications déployées au début de la crise. Les entreprises souhaitant aller plus loin que la visioconférence attendront, elles, un accompagnement pour s'approprier véritablement ces nouveaux outils.

Olivier Rafal rappelle cependant que les organisations devront faire des choix budgétaires. Le cabinet anticipe en effet une baisse des dépenses IT en 2020 comprise entre 3 et 12%. *"Un certain nombre de choix stratégiques vont devoir être faits dans les entreprises"*, avec des effets probables sur l'équipement.

"Même si tout le monde a bien conscience de la nécessité de revoir cet équipement informatique, les contraintes budgétaires sont bien réelles (...) Les nouvelles méthodes de travail, c'est assurer la résilience des entreprises et répondre aux attentes des collaborateurs, mais cela ne créé pas immédiatement de la valeur" conclut le vice-président de PAC.

LES NOUVEAUX MODES DE TRAVAIL À DISTANCE S'ANCRENT EN ENTREPRISE

Parfois proscrit ou simplement toléré, le télétravail s'est généralisé durant le confinement. La crise a été l'occasion d'apporter la preuve de son efficacité, comme de celle des outils collaboratifs et digitaux. La sortie de crise sera donc consacrée à la recherche d'un nouvel équilibre.

Selon une étude de Terra Nova conduite en avril, le télétravail a été une révolution pour une part conséquente des salariés français. **42% des répondants ont ainsi découvert le travail à distance à l'occasion du confinement.** Pourtant, un accord d'entreprise sur le télétravail préexistait dans leur organisation pour plus de la moitié d'entre eux. C'était notamment le cas au sein de Cadremploi, une entreprise spécialisée dans le recrutement sur Internet. Un premier accord sur le télétravail a ainsi été formalisé en 2017 avec les organisations syndicales. Il a été complété par la suite en 2018 et 2019.

Un avenant télétravail pour un tiers des salariés de Cadremploi

"Depuis 2019, nous avons un accord extrêmement ouvert sur l'organisation en télétravail. Grâce à ce cadre, nous avons pu assouplir au fil du temps. En 2017, il avait fallu beaucoup rassurer le management. Mais en 2020, à la veille de la crise sanitaire, un tiers déjà des collaborateurs disposaient d'un avenant formalisant une à deux journées de télétravail par semaine" détaille sa DRH, Lise Ferret.

Pour un autre tiers des salariés, le recours au télétravail était plus *"exceptionnel"*. Le tiers restant a lui *"dû être embarqué très rapidement."* Basculer l'ensemble des équipes en travail à distance représente cependant un changement radical d'échelle. Et cela suppose au préalable la formation des managers, souligne la DRH.

Ce volet était prévu dans l'accord télétravail de 2017. L'entreprise a néanmoins mené de nouvelles actions de formation au cours des 10 premiers jours du confinement. La finalité était une sensibilisation aux bonnes pratiques, notamment en termes de rituels à mettre en place. L'accord prévoyait d'ailleurs une charte des bonnes pratiques.

Les outils sont également importants, insiste Lise Ferret. Cadremploi a complété son équipement, en particulier sur la partie visioconférence. *"Nous disposions déjà de Slack pour faire des visios. Nous avons néanmoins aussi déployé Google Meet en un week-end pour multiplier les canaux et s'assurer de pouvoir couvrir les différentes tailles de réunion"* témoigne-t-elle. Les tableaux de bord, plutôt une pratique produit, présentent eux aussi un intérêt pour le suivi des missions. Des logiciels comme Trello et Monday répondent à ces besoins, surtout dans un mode 100% à distance.

Pérenniser à présent de "belles avancées"

Pour Lise Ferret, il importe désormais de *"positiver sur ces belles avancées"* introduites dans l'organisation du travail à l'occasion du confinement. La DRH anticipe un développement du télétravail avec la disparition des dernières réticences qui pouvaient être exprimées par des managers.

Au sein du cabinet de conseil en stratégie Square, la posture à l'égard du travail à distance a ainsi radicalement changé. *"Les pratiques de télétravail étaient inexistantes. Ce n'était pas dans la culture d'entreprise. Ce n'était pas non plus, ou peu, dans la culture d'entreprise de nos clients"* témoigne Vincent Canchon, directeur général en charge des opérations chez Square.

Il revendique néanmoins une adaptation rapide à cette situation inédite, au travers notamment de la publication de guides de bonnes pratiques du télétravail et du management pour l'accompagner. Cette adaptation s'imposait pour *"maintenir la vie de l'entreprise, poursuivre les travaux de nos communautés d'experts ou assurer la dispense de notre programme annuel de formations."*

Pour les décisions de direction et de management ont par exemple été mises en place deux réunions quotidiennes en visioconférence. Et preuve que les évolutions adoptées lors du confinement sont amenées à s'inscrire dans la durée, ces rendez-vous seront conservés après la crise.

"J'ai vu tout de suite l'opportunité qu'il y avait à ancrer dans les esprits le fait que les fonctions de management ne nécessitaient pas systématiquement la présence physique de tous les invités dans une même salle" déclare Vincent Canchon. Les participants interviennent désormais lors de ces rendez-vous depuis différents lieux. La raison : gagner en temps et en efficacité en apportant plus de souplesse, *"un enjeu majeur pour le futur"* insiste le dirigeant.

La souplesse : un enjeu pour le futur

"La question fondamentale n'est plus où tu es, mais où tu en es. Où tu es, c'est désormais une question du passé. Cette crise va bousculer de vieilles habitudes et nous obliger à repenser nos pratiques managériales", poursuit-il. L'organisation du travail au sortir de la crise introduira donc une plus grande souplesse, via notamment la prise en compte d'une dose de travail à distance. Ces évolutions sont présentées comme bénéfiques à la qualité de vie au travail, mais sources également d'une amélioration des performances.

Pour Lise Ferret, le principal chantier consistera à trouver un équilibre en le tout distant et le tout présent. Ce point est aussi souligné par Vincent Canchon.

> *" Il faut trouver le moyen de continuer à créer du lien et un sentiment d'appartenance à l'entreprise dans cette nouvelle organisation."*

Dynamique de groupe, qualité de vie en télétravail, préservation de la frontière en vie personnelle et professionnelle sont d'autres points d'attention à prendre en compte.

Mais la crise du Covid a également mis en évidence la nécessité de repenser le lieu de travail. Chez Cadremploi, des salariés ont ainsi déjà exprimé le souhait de se délocaliser hors de Paris, où se situe le siège.

> *"Nos espaces de travail, nous allons devoir les raisonner avec une modularité plus forte et une capacité d'aménagement encore plus agile."*

Et cela aura un impact sur les m^2 de bureaux nécessaires. Ce paramètre sera pris en compte lors du déménagement de la société, prévu en septembre.

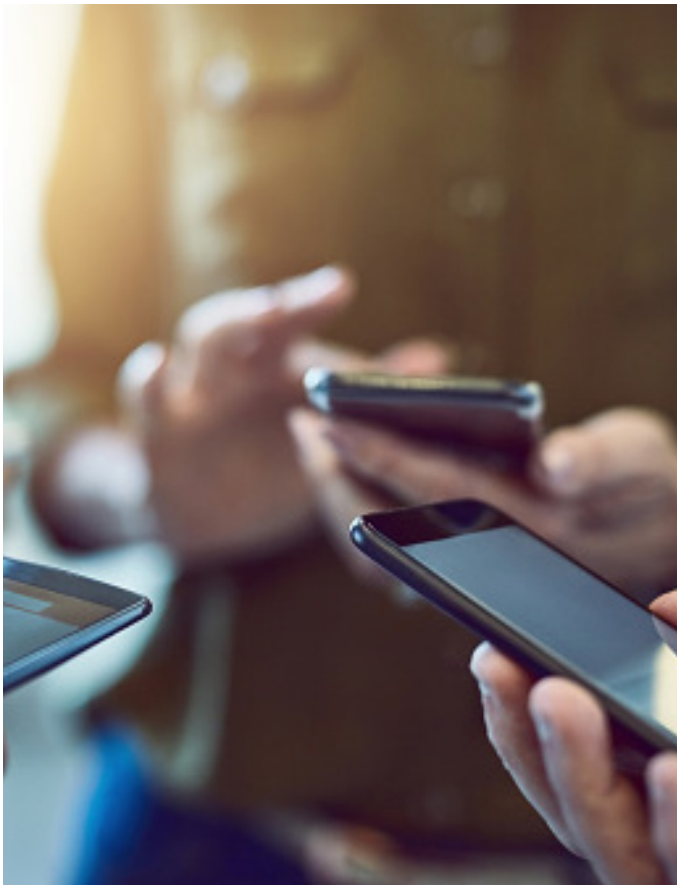
D'autres entreprises anticipent une baisse de la superficie des bureaux pour intégrer le télétravail et le recours par certains collaborateurs à des espaces de coworking. *"Je ne vois pas comment les directions générales et financières des grands groupes ne profiteraient pas de l'occasion pour rationaliser leurs dépenses immobilières et énergétiques"*, pointe le directeur général de Square.

SMARTPHONES ET APPS, OUTILS COMPLÉMENTAIRES EN MOBILITÉ CONFINÉE

Le confinement a décrété la réduction voire la fin de la mobilité. Et aussi du smartphone ? Des usages professionnels se sont déplacés vers l'ordinateur portable, et d'autres se sont développés. Mais avec un taux d'équipement en smartphone de 95%, le mobile reste ancré dans les habitudes.

Dans son enquête *"La révolution du travail à distance"*, Terra Nova estime que 8 millions de salariés français ont été convertis *"soudainement"* au télétravail durant la crise sanitaire. A titre de comparaison, ils étaient en temps normal 1,8 million à le pratiquer sur au moins 20% de leur temps de travail.

Pour permettre la continuité de leurs activités, les entreprises ont donc équipé en masse de nouveaux collaborateurs, essentiellement en ordinateurs portables. *"Nous avons équipé de nombreux salariés en portables, et véritablement tous les métiers, dont des comptables et des personnels des centres d'appels"* confie ainsi le DSI de Carglass, Didier Roy.



La visioconférence prend son essor aussi sur mobile

Mais quid du smartphone et des applications mobiles ? Les usages professionnels de ces terminaux, comme la messagerie, concernent en effet principalement les situations de mobilité. Or cette mobilité disparaît en confinement. Une part conséquente des tâches s'est donc déplacée du mobile vers l'ordinateur, pro ou personnel.

Certains usages ont néanmoins persisté sur smartphone, voire ont explosé. C'est notamment le cas de la messagerie et de la visioconférence, particulièrement adaptées à ce terminal, notamment pour les salariés non équipés de webcam. Pour organiser des réunions, les entreprises se sont massivement équipées en services cloud de visioconférence, comme Google Meet, Zoom ou Microsoft Teams. Or ces services sont déclinés en versions Web et mobiles (iOS et Android). Au début du confinement, le nombre de sessions mobiles de Microsoft Teams a bondi au-delà des deux millions pour les seuls US selon Apptopia. Google Meet a suivi une tendance similaire.

Pour Zoom, la trajectoire est encore plus brutale avec des sessions mobiles multipliées par trois à plus de 6 millions par jour. Les applications collaboratives et de visio sont indéniablement les grandes gagnantes du basculement général en télétravail. Fin avril, Microsoft annonçait ainsi que Teams comptait 75 millions d'utilisateurs actifs (44 millions six semaines auparavant). *"Nous avons enregistré sur Teams un pic de plus de 200 millions de participants à des réunions virtuelles sur une journée ce mois-ci, générant plus de 4,1 milliards de minutes de meetings"* n'a pas manqué de se féliciter son PDG, Satya Nadella.

La problématique de la sécurisation du BYOD ressurgit

Carglass fait partie de ces entreprises qui ont développé leur utilisation de Microsoft Teams. Si l'outil était déjà disponible en interne, il était cependant négligé par une part des collaborateurs.

"Nous n'avons fait qu'intensifier l'usage. Et les récalcitrants s'y sont mis eux aussi (...) Des réunions jusqu'à 50 personnes ont été organisées sur Teams" témoigne Didier Roy.

Mais que ce soit pour une visioconférence ou accéder en VPN à une application d'entreprise, les salariés ne disposent pas tous d'un terminal professionnel.

> *"Toutes les sociétés ont bien conscience de la nécessité de revoir cet équipement, mais des contraintes budgétaires se posent."*

Expert en sécurité pour Wavestone, Gérôme Billois insiste lui aussi sur la fourniture de matériel informatique. *"C'est dangereux d'autoriser l'accès au réseau interne à des PC susceptibles d'être utilisés le soir par des adolescents pour télécharger des jeux ou des séries. La journée, sur le même PC, seront tapés des emails professionnels sensibles."*

La pratique sécurisée du BYOD reste complexe à mettre en œuvre, juge-t-il encore. *"Pour les PC, c'est très difficile de mesurer véritablement la conformité d'une machine avant sa connexion"* précise le consultant. *"Dans un contexte terminaux mobiles, on arrive quand même à faire mieux avec des containers"* à la mode BlackBerry ou Knox.

Ces outils de sécurité sur mobile peuvent s'imposer lorsque le terminal combine usages pros et persos. Or, c'est surtout dans ce second domaine que les usages se sont le plus intensifiés en confinement. En effet, applications mobiles de messagerie et réseaux sociaux ont, elles aussi, enregistré un pic d'activité lors de cette période. *"Facebook, WhatsApp, Messenger, Instagram, TikTok, Snapchat et Twitter ont tous battu leurs records respectifs pour le temps passé dans l'application"* relève Apptopia.

Messagerie et réseaux sociaux font la loi sur mobile

Toutefois, ces applications étaient déjà incontournables sur smartphone avant le confinement. Chez les 20-29 ans, Facebook, Instagram, Snapchat, Messenger et YouTube s'imposent comme les principales apps selon le baromètre des usages mobiles de l'EBG. Et parmi les 30-39 ans, Google et Gmail se substituent à Snapchat et YouTube.

La crise sanitaire s'est donc traduite avant tout par une intensification d'usages existants. Mais l'attachement au smartphone et aux apps n'a en effet pas concerné tous les domaines. Pour le New York Times, ces journées au domicile, avec des ordinateurs à portée de main, ont même conduit une part significative des mobinautes à se détourner de cet écran, leur en préférant un plus grand.

C'est vrai, en partie du moins. Un indicateur permet en effet de confirmer que le Web n'est pas devenu spécifique au PC. Airship note ainsi que les notifications push sur mobile ont augmenté de 16% en mars, contre +36 % pour le Web. La tendance est similaire en ce qui concerne l'ouverture (+22% pour les applications et de 119 % pour les sites Web).

Toutefois, **88% des ouvertures directes de notifications Web provenaient d'appareils mobiles plutôt que d'ordinateurs de bureau** - soit une augmentation de 10% depuis janvier 2020 et de 42% en cumul annuel. Même confinés, les internautes n'ont pas renoncé au smartphone, même si le lien a parfois pu donner l'impression de se distendre.

La reprise progressive de l'activité dans le cadre du déconfinement devrait d'ailleurs redonner à ce terminal toute sa place. Rappelons ainsi que selon le Baromètres du numérique, tous les principaux usages du smartphone sont en constante progression année après année. Et cela s'explique par un fort taux d'équipement des Français (95%). En outre, 94% des personnes équipées l'utilisent chaque jour.

> *"51% de Français se connectent au Web d'abord sur mobile."*

L'année dernière, cette part a progressé de 5 points. Pour l'accès à Internet, le smartphone devance ainsi l'ordinateur de 20 points. L'ancrage de ce terminal n'est pas remis en question, y compris par la crise sanitaire.

CAS PRATIQUE : L'ÉVÈNEMENTIEL ACCÉLÈRE SA TRANSFORMATION DIGITALE AVEC L'HYBRIDATION

Contraint au silence par le confinement, le secteur de l'évènementiel a dû basculer à 100% en ligne. La crise joue par ailleurs le rôle d'accélérateur de la transformation du digital de ces entreprises, dont certaines préparent déjà la 3ème ère de l'évènementiel au travers de salons hybrides.

Le commerce n'est pas le seul secteur à pâtir des mouvements sociaux et depuis mars de la crise sanitaire. Le confinement a ainsi signé l'arrêt total des salons et conférences, notamment dans le B2B. Acteurs de l'évènementiel et entreprises ont dû chercher des solutions pour assurer une forme de continuité d'activité.

La crise pourrait d'ailleurs être le point de départ d'une vaste transformation digitale de l'univers de l'évènementiel. Pour le think tank HUB Institute, la crise a mis en lumière la nécessité pour le secteur d'entrer dans la *"3ème ère de l'événementiel BtoB."* Ce concept est détaillé dans un manifeste.
La 3ème ère pour Vincent Ducrey, cofondateur et PDG du HUB Institute, c'est celle de l'hybridation du offline et du online. Le 100% en ligne s'est imposé comme adaptation à la crise.

Dès la mi-mars, le think tank a basculé totalement sur Internet au travers d'un programme de webinars (Business Recovery Challenges). Le 25 juin, se déroulera en outre son premier salon en ligne *"DATA & AI for Marketing."*

Ce virage contraint a permis à l'entreprise de réunir sur Internet plus de 5000 cadres d'entreprise, touchant une audience plus importante que son public habituel.

> *"Notre communauté a basculé en ligne. Et des partenaires technologiques, qui nous connaissaient sur le monde physique, se sont tout naturellement tournés vers nous dans le monde en ligne."*

Le dirigeant du Hub Institute pose cependant une première condition à une adaptation réussie : une marque forte. La seconde serait d'avoir déjà entamé une transformation digitale, avec par exemple la diffusion en streaming des évènements physiques et des webinaires. *"Pour ceux qui n'ont pas encore démarré, ce sera très difficile. Dans l'évènementiel, il y a des acteurs qui ont effectué une transformation choisie. Depuis des semaines, des mois ou des années, ils travaillent à cette hybridation. Et il y a ceux qui devront passer par une transformation subie"* prévient-il encore.

Du côté du groupe Figaro, l'hybridation est bien au cœur des réflexions du moment. L'organisateur des salons Figaro Etudiants dans le B2C et RENT pour l'immobilier B2B planche sur sa future plateforme en ligne. Et la crise a fait office d'accélérateur. *"Ce qui s'est imposé à nous a accéléré la réflexion. Les outils virtuels qui existent, et ceux amenés à apparaître, permettent de proposer un prolongement ou une complémentarité à l'évènement physique"* témoigne Béatrice Louis, commissaire des salons pour le Figaro.

Et les bénéfices de cette hybridation sont tangibles, y compris en termes d'empreinte carbone. La combinaison avec le digital (chat, streaming, webinaires…) permet notamment d'envisager de toucher une audience plus large. Organisés à Paris, les salons Figaro Etudiants s'ouvriront aux étudiants et parents en province, voire à l'étranger.

La valeur de l'hybride, c'est bien l'engagement, appuie Vincent Drucrey. Mais attention, ***"il ne s'agit pas de remplacer l'évènement physique"*** insiste bien Béatrice Louis. Le cœur de métier de l'événementiel, c'est la mise en relation, avec donc des moyens physiques et digitaux. Elle n'oublie pas non plus le nécessaire volet d'accompagnement à destination des clients et partenaires, habitués par exemple à acheter des mètres carrés sur les salons.

Le Figaro est d'ores et déjà engagé dans ce chantier. Cette période de l'année est en effet critique pour son audience étudiante. Les étudiants devront en effet cet été statuer sur la suite de leur parcours scolaire. ***"Nos équipes imaginent les moyens de porter à leur connaissance des conférences et webinars, mais aussi de répondre à leurs questions"*** annonce la commissaire de salons.

Le cofondateur du Hub Institute insiste à ce titre sur la nécessaire extension de compétences des acteurs de l'évènementiel. ***"Le monde qui vient valorisera encore plus ceux qui codent" avec la capacité d'agréger des familles de plateformes (rendez-vous d'affaires, diffusion en ligne, multisessions…). "Aujourd'hui, aucun outil sur le marché ne permet d'offrir tout cela. Je vais donc agréger des plateformes technologiques en fonction de l'angle recherché pour mon l'évènement B2B"*** précise Vincent Drucrey.

Pas question cependant de redévelopper des solutions, notamment en raison de la rapide évolution des usages. L'agence de conseil Data Artefact n'a d'ailleurs pas réinventé la roue pour assurer sa visibilité en ligne lors de la période de crise. Sa directrice marketing, Sophie Huss, est repartie de l'outil vidéo utilisé en interne pour proposer des séminaires en ligne.

Artefact organise ainsi depuis mars 1 à 2 webinaires par semaine diffusés dans différents pays et réunissant entre 40 et 50 personnes chacun, dont 50% de nouveaux contacts. Ces activités en ligne, nouvelles pour la société de conseil, lui permettent donc de générer des leads et de développer sa notoriété.

L'hybridation est aussi en réflexion chez Artefact ***"avec quelques grands évènements en présentiel et en complément d'autres avec des approches studio en mode hybride"*** anticipe la responsable marketing. Il est par ailleurs déjà prévu de poursuivre les webinaires sur le 2ème semestre 2020, avant de mettre en place un équilibre entre le digital et le présentiel. Et le budget salons devrait par conséquent évoluer l'année prochaine.

MOBILE WORKPLACE : LE BUREAU RÉINVENTÉ SOUS LE SIGNE DE LA PRODUCTIVITÉ

Nous l'avons vu : les modes de travail évoluent, de nouveaux outils mobiles apparaissent et les attentes des salariés ont changé. Les collaborateurs travaillent de plus en plus vite et efficacement, sont connectés en permanence, mais passent de moins en moins de temps derrière leur bureau. L'environnement de travail se doit aujourd'hui d'être flexible, connecté et accessible à tout moment. En mettant en place ce nouveau système, les entreprises offrent à leurs salariés une meilleure expérience collaborateur, dynamique et innovante. Les informations se partagent plus vite, plus facilement, avec des outils qui sont aujourd'hui utilisés dans la vie quotidienne, dont le smartphone est le fer de lance. En mettant en œuvre un "mobile workplace", le collaborateur est replacé au centre de l'organisation du travail et gagne en agilité et en productivité.

DISTANCIATION PHYSIQUE AU BUREAU : LES ASCENSEURS POUR MONTER, LES ESCALIERS POUR DESCENDRE.

Le retour au bureau avec les contraintes de la distanciation physique oblige à reconfigurer l'espace disponible, tout en l'élargissant à des lieux sous-utilisés. Le point en exemples sur ces mutations compliquées à mettre en œuvre.

L'annonce du déconfinement a conduit les entreprises, quelle que soit leur taille et leur activité, à réorganiser leur lieu de travail. S'agissant des organisations ou des services travaillant sur des postes de travail (bureautiques par exemple ou applications métiers) ou encore de développement sur stations de travail, il faut impérativement installer un espace minimal de 4m² par collaborateur. Dans beaucoup d'open space, les personnes ont l'habitude de travailler quasiment côté à côté.

Selon les premiers témoignages que nous avons recueillis, les 4 m² imposés sont trop exigus. Conséquence, nombre de responsables de sites ont été contraint de calculer plus large la plupart du temps, car il faut également prévoir les passages voire un sens de circulation des personnes.

Une organisation des présences en rotation

D-Edge, société de service IT, s'était déjà bien préparé en amont de la réouverture des locaux. Mais la culture de l'entreprise a bien aidé. Beaucoup de collaborateurs - développeurs et pilotes de projets par exemple, ont une expérience internationale, *"très connectée"* par petites équipes agiles de dizaines de personnes. Surtout, elles sont rompues au télétravail, avec un rythme d'au moins un jour par semaine pour tout le monde.
Ce qui a changé ? *"Nous ferons plus de rotations en maintenant une partie des effectifs en télétravail.*

Comme il n'est pas possible dans l'immédiat de parler d'agrandissement des locaux (moins de 1 000 m²) - notre open space a une capacité de 80 personnes - il n'était pas question de réintégrer tout le monde", explique Antoine Buhl, CTO de cette SSII.

"Vu notre croissance, il n'était déjà plus possible depuis un certain temps de réunir tout le monde. Tous nos kick-offs se déroulent à l'extérieur. Les équipes étant très autonomes, elles s'organisent donc pour faire leur point hebdomadaire et tenir leurs 'sprints' toutes les deux semaines avec une partie des personnes en visio". La nouvelle organisation a cependant exigé quelques modifications supplémentaires.
"Nous avons institué la location d'espaces de coworking pour nos petites équipes installées en province, par groupe de 3 à 4 personnes. Nous avons signé pour des locaux de 4 places avec les nouvelles consignes de distanciation mais nous pouvons étendre la capacité à la demande, par exemple à Nantes et à Bordeaux."

Plutôt 10 m2 que 4 m2 ...

Chez Eni Gas & Power France - filiale du géant italien de la pétrochimie (ENI) - on n'a pas perdu de temps non plus. Dès avant le 11 mai, le responsable HSE (Hygiène, santé et environnement), l'équipe RH et les services généraux ont travaillé sur le plan de *"déconfinement"*.

Une cellule de crise avait été mise en place (la compagnie étant certifiée OHSAS 18001) ; c'est elle qui a défini le réagencement des locaux et l'application des mesures d'hygiène et les barrières sanitaires avec distanciation entre les personnes. Il a été décidé d'élargir la surface minimale de 4 m² par personne à 10 m².

"Nous avons commencé les premiers jours avec un quart des effectifs en rotation, soit une présence des personnels d'un à deux jours au maximum par semaine", explique Daniel Fava, DG d'Eni Gas & Power France.
Tout un ensemble de consignes a été appliqué notamment pour réorganiser le flux des personnes afin que les distances minimales soient préservées et que l'on se croise le moins possible.

Ainsi, les ascenseurs sont utilisés uniquement pour monter ; et les escaliers pour descendre.

"Les salles de réunion ont été ouvertes à condition que le nombre d'utilisateurs ne contrevienne pas à la distance minimale à maintenir entre eux. Et nous avons fait en sorte de faciliter la tenue de réunions de travail à la fois sur site et en télétravail en créant des espaces dotés d'écran de visioconférence."

Comme dans beaucoup d'autres firmes, les espaces cafétérias ont été fermés. Le CSE a préconisé d'éteindre les machines à café, sources potentielles de contamination. Les services d'entretien de surfaces ont été renforcés et les équipes procèdent à deux passages par jour pour la désinfection des espaces de travail - qui doivent être les plus dégagés possible.

"Nous étions préparés à une telle situation depuis deux ans, à cause du mouvement des "gilets jaunes" et des grèves de ces derniers mois", ajoute Daniel Fava. Enfin, les équipes ont été incitées à organiser elles-mêmes des rotations entre personnels sur place et en télétravail. Pourquoi ? Parce que la preuve a été faite que 90% de l'activité pouvait être gérée en télétravail.

Les expériences positives du nomadisme

Reste qu'une bonne partie du travail dans les sociétés ne s'effectue ni dans les bureaux ni à la maison. Et ce depuis longtemps. Les commerciaux ou les responsables de maintenance sur le terrain, ont dans de nombreuses organisations appris a rester connecté lors de leurs déplacements. Beaucoup utilisent par exemple les salons VIP des gares et aérogares, où avec leur smartphone ou leur laptop, ils bénéficient d'une connectivité généralement satisfaisante. Et ce genre de pratique devrait se poursuivre avec les encouragements de l'écosystème du transport dans cette période post-confinement. Ainsi pour la réouverture de l'aéroport d'Orly le 26 juin, ADP a prévu un réagencement de ses espaces VIP afin de *"redonner confiance aux voyageurs".* Un ensemble de dispositifs figure dans un rapport remis à Augustin de Romanet. Il en est de même pour les accès aux espaces réservés des TGV de Oui.SNCF, Eurostar et Thalys.

Les limites du télétravail

Pour autant, le télétravail en continu ou à 100 % n'est pas la panacée et n'est ni souhaité par les directions, ni par les salariés.

"Si le télétravail est une réalité depuis les années 90 dans certains pays, dont le Royaume-Uni ou la Silicon Valley, ce n'est pourtant pas la panacée", insiste Yann Gourvennec, CEO de Visionary Marketing et co-auteur du tout récent ouvrage collectif *"Le confinement expliqué à mon boss."*

"Nous avons sans doute 25 ans de retard. Mais là on vient de découvrir qu'il pouvait y avoir du télétravail imposé, obligatoire ! - et ce même chez vous ou près de chez vous, vous ne disposez d'un espace de travail adéquat (présence des enfants, nombre de pièces insuffisant, etc.) ou correctement connecté à Internet et en téléphonie (fixe ou mobile). Et fait, 12% de la population n'aurait pas accès à Internet de façon opérationnelle". On n'ose donc imaginer en conséquence les chiffres de la mobilité pour les professionnels.

> *" En clair, le télétravail ne devrait pas être tout le temps ni pour tout le monde car pas adapté à tous les jobs, ni à tous les tempéraments."*

Quant à la configuration des bureaux, après le confinement, certains s'interrogent : les open-spaces sont-il pérennes ? Les flex-offices ont-ils vraiment leur raison d'être ? Certains grands groupes, qui occupent des tours par exemple à la Défense, ont déjà laissé filtrer l'idée que les surfaces de bureaux seraient reconsidérées, si elles ne s'avéraient plus indispensables.

TÉLÉTRAVAIL, NOMADISME, FLEX OFFICE / SMARTPHONE, TABLETTE, PORTABLE, TERMINAL VDI ; EXISTE-T-IL UN POSTE DE TRAVAIL UNIVERSEL ?

Le recours au télétravail intensif a reposé la question du poste de travail. Y-a-t-il un terminal universel ? Idéalement, certains utilisateurs voudraient combiner PC portable ou terminal VDI, smartphone ou tablette... Que faire ?

Contraintes à généraliser le télétravail à l'issue de la période de confinement, les entreprises et les administrations ont eu quelques jours à peine pour répondre à une question critique : de quel poste de travail peuvent disposer les collaborateurs.

Pour les services où l'utilisation d'un PC était de rigueur, c'est le portable qui s'est confirmé comme la réponse universelle. A tel point que dans les banques ou les administrations où les postes de travail étaient encore des postes fixes à quelques jours du confinement, il a fallu vider les stocks de 'laptops' disponibles et se hâter d'en commander par dizaines ou centaines voire par milliers, dans les plus grandes organisations.

Or, les livraisons en provenance de la principale source d'approvisionnement - la Chine - se sont vite taries ou ont été considérablement ralenties, du fait de l'arrêt ou de la baisse d'activité dans les usines - ou du fait de l'interruption des transports. Heureusement, certains fournisseurs possèdent encore des lignes de production 'near-shore' en Europe.

VDI et clients légers

Autre constat : beaucoup d'organisations ne renoncent pas à utiliser des terminaux clients légers, du type Wyse, fonctionnant sur des plateformes VDI (Citrix, VMware...). Voire à positionner les VDI directement sur des portables standards.
Ces plateformes virtuelles dans cette configuration présentent un avantage : celui de pouvoir utiliser des poste hétérogènes, d'origines diverses, permettant de reprendre le principe - un peu oublié ou écarté - du BYOD (Bring your own device).

De fait, leur connexion reste subordonnée à un filtrage des accès par des couches logicielles - protocoles de sécurité et outils de management à distance (MDM). Ce qui implique beaucoup d'interventions par les équipes IT et, nécessairement, un peu d'intrusion.

Tablettes 3G/4G ou clés USB 4G sur PC portable

Les utilisateurs nomades - commerciaux, personnels de maintenance, transporteurs logisticiens... - donnent généralement priorité à l'utilisation de leur smartphone.

Mais souvent, certaines de leurs applications nécessitent d'utiliser un écran et un clavier, se seraient que pour rédiger du texte quand cela est nécessaire. Certains consultants - profession à la fois nomade et en télétravail à leur domicile comme chez leurs clients - trouvent donc fort pratique d'utiliser leur PC portable pour leurs communications téléphoniques (avec un kit oreillette, softphone). A ceci près qu'il faut nécessairement disposer d'une bonne connexion internet. Ou d'une clé USB 4G dédiée.

> *"Il est étonnant de constater que les constructeurs de 'laptops' n'aient pas maintenu cette idée d'une carte SIM 4G intégrée, comme sur les tablettes."*

Marché trop limité ou complexité de la relation avec les opérateurs mobiles ? Toujours est-il que bon nombre d'entreprises ont eu le réflexe, pour leurs collaborateurs en télétravail mal desservis en Internet, de leur procurer des clés USB 4G LTE (moins de 50€) pendant la période de confinement. Et après.

Transformer son smartphone en laptop ?

Autre cas de figure, celui des personnels nomades inconditionnels du smartphone et peu enclins à transporter un PC portable lourd et encombrant, long à se mettre en route (sous Windows, plus que sur MacBook). Que peuvent-ils faire ? Ils peuvent toujours tenter l'expérience des extensions dites 'stations d'accueil' (dock, en anglais). Elles ne datent pas d'aujourd'hui. Initialement, il s'agissait d'un socle pour le chargement de la batterie, auquel ont été ajoutées des connecteurs USB pour haut-parleur ou *"barre de son"* ou la sauvegarde sur disque externe - à l'instar des stations d'accueil des constructeurs de PC portables depuis les années 80.

Depuis deux à trois ans, à destination des smartphones, on a vu fleurir avec plus ou moins de succès des concepts plus élaborés. Une start-up française, Miraxess, a même conçu en 2018 le Mirabook, sorte de notebook sans processeur, pouvant récupérer l'écran de smartphones Android ou Windows. La percée se fait toujours attendre.

Quelques années auparavant, Microsoft avait une offre, Continuum, de déport d'écran de ses smartphones (sous Windows) vers tablette ou laptop avec clavier. L'épisode là aussi a tourné court.

DeX en pointe sur les stations d'accueil

Pourtant, il existe toujours la possibilité d'acquérir séparément des kits de station d'accueil pour smartphones, avec la capacité de connecter un écran externe, une souris sans fil et un clavier repliable (Wish, Leotec ou Jelly Comb...) ou des claviers/touchpad très compacts (comme Drumstone). A noter que, pour la France, les claviers Qwerty ne feront pas l'affaire...

Pour l'affichage, il convient de vérifier que le format se reporte bien (homothétie) et que sa taille et sa résolution soient au moins égales à celles du smartphone. Pas de soucis majeurs, en revanche, avec la souris - sauf avec certaines 'mobile-apps' (transposition du tactile en boutons cliquables, gestion des ascenseurs, etc).

Dans ce registre, Samsung est l'un des rares constructeurs à détenir, depuis deux ans, une solution de ce type : sa station de base DeX reste compatible avec ses Galaxy de dernière génération. Compacte (10 x 10 x 5 cm pour 230 g), elle permet, pour moins de 100 euros, de brancher un écran (HDMI), un clavier, une souris (Bluetooth ou 2 ports USB), tout en intégrant un chargeur rapide et un port RJ 45 pour une prise câblée Ethernet. A noter que l'ensemble des appareils premium de Samsung, permet de se passer de dock en branchant simplement le smartphone via une connectique USB C ou USB A.

Il est donc possible de connecter le Dex Pad à un écran plat à la dimension de son choix, sans redémarrage. On peut choisir le mode miroir d'écran (report) de son smartphone ou le mode DeX (écran virtuel). Plusieurs fenêtres peuvent être ouvertes. La barre des tâches permet de lancer des appels téléphoniques, d'écrire des SMS avec le clavier ou de lancer toutes autres applications (bureautiques, métier, navigation sur le web, recherches géolocalisées, etc.) comme sur un PC portable. Il reste à vérifier que toutes les applications que l'on utilise soient compatibles avec l'écran virtuel DeX.

La téléphonie DECT subsiste

A noter enfin que beaucoup d'organisations continuent de gérer leur mobilité, et les applications y afférant, autour d'un IPBX et de centres d'appels, souvent avec serveurs vocaux. La crise du Covid-19 a rappelé que dans les établissement de soins, dans les services d'urgences, les secours etc, la téléphonie reste primordiale. Il reste là encore à maintenir et enrichir les passerelles entre ces univers et ceux des 'mobil-apps' – tout en intégrant des systèmes voix et données pour appels de groupes (MCPTT, Mission Critical Push to Talk) qui tirent parti des infrastructures 4G LTE et demain de la 5G.

5 ASTUCES POUR GARDER LE CONTACT AVEC SON ENTREPRISE, MÊME CONFINÉ !

Assurer aux collaborateurs des conditions optimales pour remplir leurs missions à distance… Un défi ? Non, une méthode qui exige de s'appuyer sur des solutions nativement orientées sur l'ergonomie et la sécurité. Durant le confinement, les utilisateurs des équipements Samsung ont ainsi pu bénéficier des fonctionnalités innovantes de ses produits, mais également des solutions B2B qui y sont associées. 5 conseils clés pour tirer le meilleur du travail à distance.

Conseil N°1 : Créez les conditions de sécurité optimales pour l'ensemble de vos terminaux mobiles

À l'annonce du confinement par le Gouvernement, les entreprises n'ont eu finalement que 72 à 96 heures pour réagir et réinventer de nouveaux modes de travail à distance, avec pour priorité la nécessité de garantir la productivité des collaborateurs dans des conditions de sécurité optimales. Face à cette réalité, les entreprises qui avaient déjà déployé Samsung Knox pour administrer les terminaux des collaborateurs ont eu un avantage certain ! *"Avec Samsung Knox, les protocoles de sécurisation sont directement intégrés dans les terminaux, explique Adrien Pacgep, B2B Technical Product Manager Samsung Knox, créant ainsi les conditions nécessaires à des usages professionnels en situation de mobilité"*.

Conseil N°2 : Basculez en mode DeX pour une expérience optimale des plateformes collaboratives

Le principal effet du confinement aura été de resserrer les liens virtuels entre les collaborateurs qui se sont massivement orientés vers les plateformes collaboratives. Toutes ont explosé : Zoom revendiquait ainsi près de 300 millions d'utilisateurs quotidiens fin avril, contre seulement 10 millions en décembre dernier. La solution Microsoft Teams a franchi le cap des 75 millions d'utilisateurs quotidiens, contre 32 millions au 11 mars et Slack totalisait 12,5 millions d'utilisateurs à la fin du mois de mars, soit une augmentation de 2,5 millions en un mois ! Les collaborateurs dotés d'un smartphone Samsung, pouvaient, en basculant en mode DeX, disposer via leur terminal mobile et d'un moniteur d'une expérience 100% comparable à celle qu'ils auraient connue sur un PC. *"Le mode DeX préserve l'ergonomie des interfaces des applications sans intervention de l'utilisateur, pour une productivité optimale en toutes circonstances"*, précise Adrien Pacgep.

Conseil N°3 : Déportez votre téléphonie fixe sur vos terminaux mobiles

La productivité des collaborateurs, lorsqu'ils sont à distance, ce n'est pas seulement la dimension collaborative, c'est aussi la joignabilité ! La mise en œuvre d'une véritable stratégie de télétravail à l'échelle de l'entreprise doit en effet être bien préparée et inclure un accompagnement spécifique pour que chacun y trouve matière à y exprimer tout son potentiel.

> *"La transition du fixe vers le mobile est l'un des points à suivre de près afin de garantir la continuité du service."*

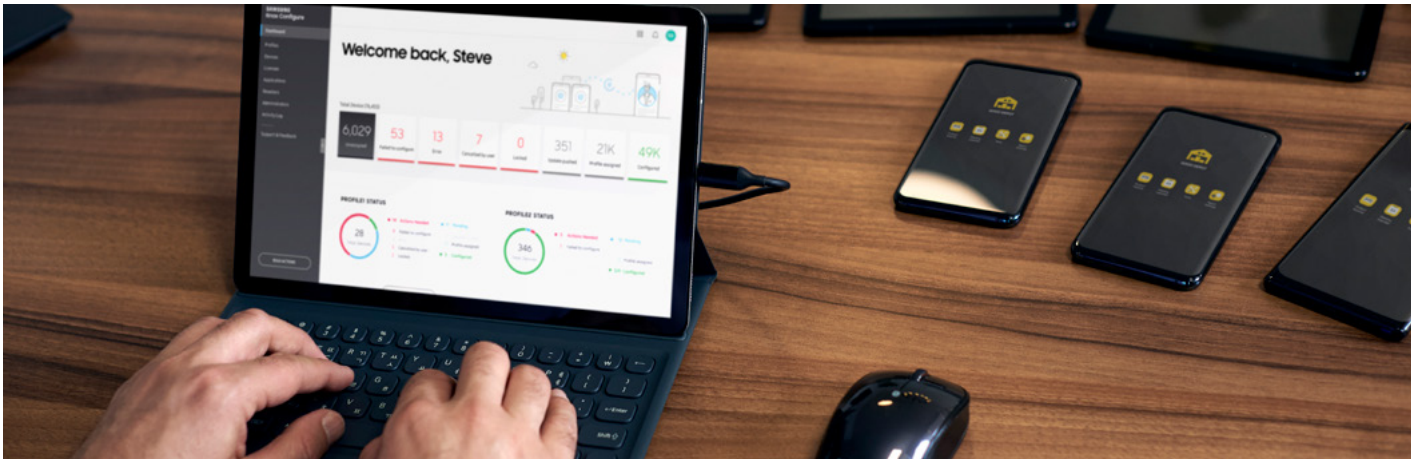
"Associé à DeX, cela permet par exemple de prolonger l'expérience collaborative via Teams, Slack ou Zoom sur l'écran, tout en répondant à un appel téléphonique reçu sur le mobile", observe Adrien Pacgep.

Conseil N°4 : Gardez le contrôle pour résoudre les problèmes à distance

Lorsque les équipes sont disséminées aux quatre coins d'un territoire, il est capital d'assurer une expérience optimale même à distance, et de résoudre les problèmes techniques quand ils se présentent. **Avec Samsung Knox et les fonctionnalités de Remote Control,** précise Hamdi Abed Channel Technical Account Manager chez Samsung France *"les responsables informatiques sont en mesure d'anticiper les difficultés et d'assurer l'entretien constant de leur parc, sans intervention physique sur les terminaux. Un moyen efficace de garantir la continuité de l'activité !"*

Conseil N°5 : Optimisez la sécurisation à la carte

La sécurisation des terminaux est au cœur de la réponse Samsung Knox, mais certains secteurs d'activité, certains profils de collaborateurs, exigent des niveaux encore plus élevés de protection pour garantir non seulement l'intégrité des données et des usages, mais aussi la sérénité de l'utilisateur. *"Les apports de certains partenaires, comme par exemple Ercom avec sa solution Cryptosmart, qui permet de chiffrer automatiquement les communications mobiles, permettent de dépasser le seul enjeu de sécurisation du lien physique,* confie Adrien Pacgep. *Certains pays ont choisi de sécuriser leurs flottes mobiles par ce biais pour garantir un niveau de sécurité secret défense"* ... Une sécurisation adaptable en fonction de l'enjeu !



SAMSUNG ENTREPRISE EDITION : LA SOLUTION MOBILE 100% ENTREPRISE

Véritable offre dédiée à la sécurité, à la gestion et à la personnalisation des flottes mobiles, Entreprise Edition est une solution unique sur le marché, spécialement packagée pour répondre aux enjeux des entreprises. Frédéric Fauchère, Directeur de la Division B2B Mobilité, revient sur la genèse de Samsung Entreprise Edition.

Quels ont été les principes et ambitions qui ont présidé à la conception du pack Entreprise Edition et comment se déploie-t-il concrètement sur l'offre Samsung ?

Frédéric Fauchère : Nous sommes partis du constat que les équipements mobiles se gèrent désormais de la même façon que les parcs de PC. Dans le même esprit que celui qui nous a amené à développer Knox en 2013, nous avons donc conçu en 2018 Entreprise Edition, qui est une sélection de nos smartphones et tablettes les plus plébiscités par nos clients professionnels. Cette sélection est exclusive, car nous nous engageons à conserver ces équipements à notre catalogue pour une durée de deux ans, et intégrons également quatre ans de correctifs de sécurité mensuels. Enfin, nous avons incorporé nativement à ces produits deux de nos solutions Knox : Knox Configure pour personnaliser les appareils, et Knox E-FOTA pour gérer les versions d'OS.

À quelles problématiques "professionnelles" avez-vous spécifiquement cherché à répondre ?

Frédéric Fauchère : La principale difficulté à laquelle font face les gestionnaires de parcs mobiles, DSI et RSSI, reste la complexité de déploiement, avec des modèles dont les cycles de vie – c'est-à-dire la disponibilité ou le référencement – n'excédaient pas 12 à 18 mois.

L'autre problématique essentielle, c'était l'indispensable réactivité par rapport aux failles de sécurité. Grâce à son partenariat avec Google, Samsung était légitime pour piloter cette approche sécurisée. Aujourd'hui, nous publions nos mises à jour de sécurité en même temps que Google. Enfin, les entreprises, à l'instar de ce qu'elles font avec la masterisation de leur parc de PC, étaient en attente d'une solution permettant un haut niveau de customisation (fonds d'écran, personnalisation des terminaux aux couleurs de l'entreprise, applications métiers, règles de roaming, profils utilisateurs, etc). Samsung Entreprise Edition offre une plus-value particulièrement appréciable aux équipes IT en simplifiant considérablement l'administration, le pilotage et la sécurisation des terminaux mobiles.

À vos yeux, à quel(s) profil(s) d'entreprise(s) ou de professionnel(s) s'adresse plus spécifiquement la gamme Entreprise Edition ?

Frédéric Fauchère : Dès lors qu'une entreprise se dote d'une DSI et que son effectif approche la centaine de collaborateurs :

> *"Entreprise Edition apporte une vraie réponse aux enjeux de sécurisation, de personnalisation et d'optimisation des mises à jour des terminaux."*

Mais aujourd'hui cette offre rencontre un succès autant auprès des PME que des grandes organisations, car toutes les entreprises souhaitent avoir une solution clé en main (produit + services) afin de simplifier le déploiement de la mobilité dans leur organisation.

Comment évolue et continuera d'évoluer la gamme Entreprise Edition ?

Frédéric Fauchère : Entreprise Edition va encore évoluer pour coller toujours plus précisément aux besoins de nos clients. Notre ambition est d'aller encore plus loin notamment avec Knox E-FOTA, qui permet de garantir à distance la mise à jour des correctifs de sécurité. Nous prévoyons donc, d'élargir les services disponibles à travers Entreprise Edition pour offrir plus de choix et de flexibilité.

Quand est prévue cette évolution ?

Frédéric Fauchère : Bientôt...

Frédéric Fauchère
Directeur de la Division B2B Mobilité

LA SÉCURITÉ MOBILE, PLUS QUE JAMAIS AU CENTRE DES PRIORITÉS DES ENTREPRISES

La mobilité est en pleine essor et la limitation des déplacements a augmenté l'utilisation d'applications en tout genre. Sans surprise, la croissance des usages mobiles a également ouvert les portes aux failles de sécurité. En quelques semaines, les cyberattaques ont considérablement augmenté, des ransomwares ont été téléchargés, de même que des applications de visioconférences ont laissé fuiter des données personnelles... et professionnelles. Si les entreprises ont dû se réorganiser en urgence pour travailler "comme avant", elles n'ont pas pu esquiver la mise en place de mesures de sécurité plus poussées. Les outils mobiles doivent alors intégrer directement une protection pour garantir la sécurité des données de l'entreprise et répondre à tous les niveaux d'exigences.


VPN

SÉCURITÉ EN TÉLÉTRAVAIL ET CONFINEMENT : LES ENTREPRISES INÉGALES FACE AUX RISQUES

Les organisations ne sont pas égales face aux risques de cybersécurité. Leur maturité en matière de télétravail tend à définir le niveau de menace auquel elles sont confrontées. Détails des risques et bonnes pratiques en période de crise.

Une grande part des Français a découvert le télétravail à l'occasion du confinement. Cette période s'est même prolongée jusqu'à la fin du mois de juin, à la demande des autorités. Et elle pourrait encore durer jusqu'à la fin de l'année pour une partie des collaborateurs.
Or, sécuriser données et applications dans un contexte de télétravail peut poser des difficultés aux organisations, pas toujours suffisamment préparées. Ainsi, la prise en compte de la sécurité dans le contexte de crise s'est caractérisée par une *"très forte hétérogénéité"*.

Modernes, classiques et réfractaires : à chacun un niveau de risque

Pour l'expert en sécurité de Wavestone, Gérôme Billois, ces différences d'une société à l'autre découlaient in fine *"de la posture en matière de télétravail"*. Trois grandes catégories peuvent être définies en ce qui concerne le télétravail. Et à chacune un niveau de sécurité plus ou moins important.
Les entreprises dites *"modernes cloud"*, dotées pour l'activité des salariés d'applications cloud comme G Suite ou Office 365, ont pu globalement éprouver moins de difficultés pour protéger leurs systèmes.

La sécurité est, en effet, souvent prise en compte directement dans ces outils SaaS. En outre, les organisations ont souvent déployé des solutions de protection pour accompagner ces usages Web.

Seconde catégorie, les classiques. *"Ils font plutôt du télétravail à l'ancienne avec des VPN sur des PC fournis par l'entreprise."* Pour le partner cybersécurité de l'ESN, les membres de ce groupe doivent composer avec deux *"types de soucis"* : la taille et la disponibilité des systèmes, non prévus pour accueillir autant de connexions simultanées. Cette situation a pu se traduire par *"une dégradation des niveaux de sécurité, avec par exemple la désactivation de l'authentification forte faute de licences suffisantes, ou encore de l'application des correctifs."* Mais en outre, des applications n'étaient pas accessibles par VPN. Elles ont dû être rendues accessibles rapidement néanmoins.

Des règles de pare-feu supprimées pour la continuité d'activité

> *"Nous avons vu des pans entiers de règles de pare-feu sauter pour ouvrir des univers applicatifs qui n'avaient initialement pas été autorisés en télétravail."*

témoigne Gérôme Billois. Toutefois, c'est pour la troisième catégorie de télétravailleurs que les challenges sont les plus conséquents : les *"réfractaires"*. Ces entreprises sont allées contraintes sur le télétravail. Totalement impréparées, elles ont pu opter pour une *"ouverture non maîtrisée"*. En clair : une *"situation à risque"* observe l'expert. Ces faiblesses en termes de sécurité posent naturellement des risques, y compris pour les plus avancées. Le principal porte sur les données. *"On sait que des données d'entreprise ont été sauvegardées sur des clés USB, accédées depuis des plateformes mises en place rapidement telle que Zoom. De nombreux comptes Dropbox ont été montés pour partager des documents. On a un véritable souci sur l'éclatement des données."*

Les collaborateurs doivent donc être sensibilisés à cette problématique des données pour une sauvegarde et une recentralisation sur les systèmes maîtrisés par l'IT. Elles devront ensuite être supprimées des plateformes alternatives exploitées en phase de télétravail imposé.

Les systèmes constituent le second pôle de risques. Le niveau de protection est moindre faute par exemple d'un déploiement aussi rigoureux des correctifs de sécurité.

> *"Il faut reprendre le contrôle afin d'assainir la situation. Un rattrapage sur les systèmes s'impose."*

La nécessaire recherche de menaces et d'attaques

Enfin, reste le risque de la surveillance sécurité. Les outils classiques de détection d'intrusion ou des fuites de données, par exemple, n'ont pu fonctionner de manière aussi efficace dans une configuration en télétravail, comparativement au fonctionnement sur le réseau interne. *"Nous avons observé des cas où le serveur VPN disposait d'une seule adresse en sortie. Vous vous retrouvez donc avec des milliers d'utilisateurs avec la même adresse IP. Faire des analyses fines de sécurité est forcément difficile"* rapporte le consultant.

Les actions à court terme des équipes sécurité impliqueront dès lors la recherche de menaces et d'attaques sur la période antérieure de confinement. Des grands comptes ont lancé des chantiers dans ce secteur dès le début du mois de mai. Suivra le redémarrage des processus mis en standby, comme les tests d'intrusion.

Les enjeux sont aussi sur le moyen terme. En raison du risque de survenue de nouvelles crises, les entreprises doivent désormais penser télétravail massif et sécurité associée. Gérôme Billois insiste aussi sur la gestion de la continuité des activités cyber dans un tel contexte, mais aussi la gestion d'une crise en termes de cybersécurité.

Un exemple opérationnel : une attaque par ransomware touchant les PC des collaborateurs à leur domicile. Confinement et distanciation contribuent à accentuer la difficulté de la gestion d'une telle crise. *"Personne n'y est préparé. Les grandes entreprises sont sur des phases de réflexion amont pour définir les moyens de limiter les impacts et de s'organiser."*

L'authentification forte, chantier prioritaire des "réfractaires"

Mais c'est peut-être d'abord pour les organisations *"réfractaires"* au télétravail que les chantiers de sécurisation sont les plus urgents. Pour l'expert de Wavestone, la première des priorités est indubitablement l'authentification forte. *"S'il ne devait y avoir qu'un chantier, ce serait celui-ci"* insiste-t-il.

Il préconise également l'adoption d'applications Cloud ou à défaut la mise en place d'un VPN, ainsi que la fourniture de matériel informatique aux salariés. Cela permet de prévenir les risques liés à la cohabitation d'usages personnels (voire familiaux) et professionnels sur un même terminal. Cela représente cependant un coût. Comment dès lors accompagner de manière sécurisée le BYOD ?

Le sujet est débattu depuis des années. Pour le spécialiste de la sécurité, les limites de ce modèle sont évidentes.

"Pour les PC, fixes ou portables, c'est très difficile de mesurer véritablement la conformité d'une machine avant qu'elle se connecte" juge-t-il. Sur terminaux mobiles, la réduction des risques est en revanche plus atteignable grâce par exemple à des containers de type BlackBerry ou Samsung Knox.

La sensibilisation à la sécurité s'impose aussi comme un pilier important, plus encore pour des collaborateurs en télétravail et insuffisamment sensibilisés auparavant. Conscientes de ce risque, des entreprises ont d'ailleurs lancé des campagnes de sensibilisation au début du confinement. Les réfractaires au télétravail pâtissent eux vraisemblablement de lacunes dans ce secteur.

Dernière mise en garde en termes de menaces : la reconnexion des PC d'entreprise lors du retour dans le réseau interne. Existe en effet le risque d'introduction de codes malveillants à cette occasion. *"Il y a une procédure spécifique de nettoyage à mettre en œuvre si l'entreprise ne dispose pas déjà de contrôle d'accès au réseau permettant de bloquer un terminal à risque"* conclut Gérôme Billois.

FACE AUX VPN, QUELLES ALTERNATIVES
PROXYS, SSL, LS OU OPTIONS CLOUD ?

Le télétravail "forcé" dû au Covid-19 a mis en exergue la nécessité impérieuse de sécuriser tous les accès à distance. Les solutions VPN ont souvent été généralisées dans les grands comptes. Moyennant des investissements conséquents. Que valent les alternatives, avec ou sans le Cloud ?

Pour sécuriser les accès aux applications de l'entreprise, les DSI procèdent souvent à une distinction entre la criticité des 'jobs' des salariés. Les métiers stratégiques pour l'entreprise, ceux accédant encore des serveurs de fichiers bénéficient d'une protection renforcée, avec double authentification. En général, c'est l'option VPN qui est retenue, même si cela consomme des ressources du datacentre (serveurs dédiés de préférence) et des coûts de licence.

Pour les utilisateurs orientés bureautique et consommateurs d'applications SaaS sur le Cloud (CRM comme Salesforce, RH etc), beaucoup ont retenu des alternatives telles que les proxys renforcés mais surtout les solutions propres aux applications Web et multi-cloud - avec le recours, notamment, à une authentification unique du type SSO (Single signe on), comme préconisé par Google.

Le point le plus critique reste le cas où il faut supporter des terminaux n'appartenant pas à l'entreprise - c'est l'approche BYOD (Bring your own device) de moins en moins acceptée. Car, le verrouillage du poste distant, intrusif, est difficile s'il est utilisé à titre familial à la maison - à moins d'avoir anticipé avec une infrastructure VDI (Virtual desktop infrastructure - comme HDX de Citrix - ex ICS). Ceci explique que les entreprises ont majoritairement choisi de réinvestir dans le terminal - un PC portable le plus souvent, configuré par la DSI.

La limite des solutions 'proxy'

Pour les petites structures aux données peu sensibles et avares de leur bande passante, un proxy associé à un bon anti-virus peut suffire. Il masque les adresses IP en insérant une IP anonyme. En complément, les Smart DNS ont ajouté la possibilité de supprimer les données de localisation.

Idéalement, il faudrait un chiffrement entre le poste de travail et le proxy, et les informations d'identification devraient pouvoir s'effacer après utilisation (les anti-virus le proposent).

Les proxys sont souvent gratuits. Mieux vaut s'assurer de l'intégrité de la plateforme qui les propose. Des fournisseurs comme TeamViewer proposent des solutions *"tout-en-un"* équivalente pour l'accès à distance d'un poste Windows ou Mac, à un tiers du cout d'un VPN. Elles permettent de partager des fichiers importants et d'accéder aux serveurs de l'entreprise à distance. On peut également les éteindre ou les rallumer à distance. Et une fonction écran noir, permet de cacher l'ordinateur distant. Liaisons louées, MPLS ou autres réseaux privés.

A l'opposé, certaines grandes organisations - défense, aéronautique, spatial... - ont encore les moyens de supporter le coût d'un réseau privé reposant sur des liaisons spécialisées (LS) chèrement louées aux opérateurs. C'est le cas des offres MPLS (Multiprotocol label switching). Il y a aussi le cas d'infrastructures entièrement privées sur fibre noire, typiquement des réseaux métropolitains (MAN) fermés ou PPN (Physically private networks).

La banalisation rassurante des VPN

> *"La solution VPN reste la bonne à condition que le nombre de communications simultanées soit suffisant, que l'infrastructure IT ait été suffisamment dimensionnée."*

résume Antoine Buhl, CTO de D-Edge, SSII spécialiste des technologies hôtelières et de marketing (groupe Accor).

La solution VPN (virtual private network ou réseau privé virtuel) reste très largement la plus courante et elle a largement été sollicitée par les entreprises pour généraliser le télétravail. Son avantage est de créer une connexion sécurisée quel que soit le ou les réseaux utilisés - RTC, RNIS, ADSL, Câble, Liaison radio, LS...

Des adresses IP dédiées sont fournies et le trafic est acheminé et chiffré par des serveurs spécialisés, privés et dédiés - pour des raisons de performances, selon le volume des données transférées et le nombre d'utilisateurs simultanément connectés. Plus ces serveurs VPN sont éloignés, plus les performances de connexion baissent.

La sécurité d'un VPN dépend pour une large part du niveau de sophistication du chiffrement (clés sur 256 bits, symétriques ou non, etc.). Les algorithmes de cryptographie, ou 'ciphers', incluent les algorithmes d'encryption et d'authentification. La gestion des clés est généralement assurée par un des infrastructures à clé publique, dites PKI, donnant lieu à des certificats (cf. VeriSign, Thawte... ou des SSII certifiées comme Atos, Thales). Beaucoup de fournisseurs proposent d'en assurer le service. Il suffit de leur faire confiance...

Tunnels VPN IPsec ou SSL / TLS ?

Des fournisseurs patentés comme Fortinet proposent le choix de tunnels VPN en IPsec ou SSL. Au passage, comme pour les proxys, on se méfiera des VPN gratuits dont beaucoup sont à l'origine de vols de données.

IPsec (IP security protocol, développé par l'IETF) sécurise la connexion TCP/IP par une authentification et le chiffrement des paquets IP dans un tunnel virtuel, avec échange de clés donc sur la couche 'transport'.

SSL (Secure socket layer), rebaptisé en 1999 TLS (Transport layer security), reste le protocole universel de sécurisation le plus répandu pour la navigation sur le Web. Pour rappel, HTTPS correspond à HTTP sur SSL et FTPS est une extension de FTP (File Transfer Protocol) utilisant SSL. Pour autant, SSL n'est pas compatible avec toutes les applications.

A l'inverse des tunnels IPsec, les VPN SSL sont *"clientless"* ; l'accès se fait depuis un navigateur Web, donc de façon transparente vis-à-vis du barrage des pare-feu ('firewalls').

Le 'Zero trust' en sus

Créer un périmètre sécurisé avec des pare-feu et des tunnels virtuels VPN reste une bonne solution. Mais que faire, avec les applications passées sur le Cloud à distance, hors de l'entreprise et avec des terminaux non contrôlés par la DSI ?

Les responsables sécurité invoquent le 'zero trust' - principe de la *"confiance zéro"*. En clair, il faut aussi prévoir qu'un hacker ait réussi à entrer dans un VPN. Il faut pouvoir détecter et bloquer les comportements anormaux, intrusifs - les copies de fichiers systématiques, etc.

Les Cloud VPN

Avec la généralisation des accès Cloud, les hyperscalers (AWS, Google, Microsoft Azure) proposent également leur offre alternative ou s'inspirant des VPN. Ainsi, le Cloud VPN de Google permet de constituer un ou deux VPC, Virtual Private Cloud via des passerelles VPN IPsec à l'entrée et à la sortie ("classiques" ou à haute disponibilité sur une région, avec un débit est de 3 Gbits/s par tunnel). Certains fournisseurs de VPN recommandables comme Permieter'81 proposent aussi leur VPN Cloud avec authentification unifiée SSO pour Google Suite (Google Cloud Identity), Okta Identity Cloud, Microsoft Azure AD et Active Directory / LDAP.

Citrix : une alternative Cloud sans VPN

A noter, enfin, qu'il existe des alternatives Cloud – sans VPN. C'est le cas de l'offre Citrix Access Control : elle apporte un accès sécurisé au niveau de la couche applicative. Elle est définie comme un *"service cloud entièrement géré et disponible à l'échelle mondiale"*.

SÉCURITÉ MOBILE :
PLUS QUE JAMAIS UNE PRIORITÉ

Parce que nos smartphones ne quittent plus nos poches, ils sont devenus un objet du quotidien. Au point d'en oublier les risques associés ? Explications avec Kevin Bambara, Responsable Solutions & Alliances B2B Mobile pour Samsung Electronics France.

Sous l'effet du confinement, le smartphone a joué un rôle déterminant tant pour les usages professionnels que personnels. Selon une étude réalisée par App Annie et publiée à la fin du mois de mai, **le temps moyen passé chaque jour sur un smartphone a augmenté de 25%** en France durant la période. Une réalité qui remet sur le devant de la scène l'enjeu de la sécurité mobile, car ces terminaux professionnels sont autant de portes d'entrée potentielles vers le SI des entreprises. D'autant que, selon une autre étude réalisée par Barracuda Networks, les tentatives d'hameçonnage ont augmenté de 667% entre le 1er et le 23 mars. Pour Kevin Bambara, Responsable Solutions & Alliances B2B Mobile pour Samsung Electronics France, *"depuis plusieurs années, nous avons assisté à un phénomène de transposition des pratiques de sécurité héritées de l'univers PC/IT sur le canal mobile car le smartphone constitue un prolongement naturel de l'ordinateur"*. Une évolution qui a permis une certaine appropriation des bonnes pratiques liées à la sécurisation par utilisateurs, mais *"qui a amené les fabricants de smartphones et les développeurs d'OS mobiles à concevoir des solutions et des équipements de sécurité qui ne soient pas perçus par les utilisateurs comme des contraintes qui les amèneraient à trouver des solutions de contournement"*.

L'efficacité du Security by design

Malgré cette convergence, les menaces pèsent différemment. *"L'installation d'applications tierces sur un OS mobile constitue le principal canal de compromission des données stockées sur le terminal et des données réseau. L'enjeu, c'est celui des données en transit"*, observe Kevin Bambara. L'action coordonnée des fabricants de smartphones, des fournisseurs d'exploitation mobile et des éditeurs d'applications *"ont permis d'atteindre aujourd'hui un niveau de protection très satisfaisant car inscrit dans une dimension security by design"*. L'acculturation progressive des utilisateurs par rapport aux principes de la sécurité informatique, combinée à la généralisation du SSL, au renforcement des mécaniques de certification porté par Google, ou encore au chiffrement des données stockées sur le terminal, ont été autant d'étapes importantes pour renforcer la sécurité mobile.

> *"Cette intégration native de la sécurité tant au niveau matériel que logiciel, a permis de créer un socle de base qui épargne les frictions et la complexité à l'utilisateur final, qui demeure, quoi qu'il arrive, un maillon essentiel de la chaîne de sécurité mobile. "*

Le recours à la biométrie par exemple, qu'il s'agisse de la reconnaissance d'empreinte digitale ou faciale, ou encore par le biais d'un capteur d'iris, facilite l'adoption de l'authentification à facteurs multiples, en évitant le recours systématique aux mots de passe. Plus l'expérience utilisateur est simple, fluide et satisfaisante, plus l'acceptation des mesures de sécurisation est forte. Un enjeu qui passe notamment par un important travail sur l'ergonomie des solutions contribuant à la sécurité mobile.

Knox : vecteur d'optimisation de la sécurité mobile

C'est en réponse aux inquiétudes des entreprises par rapport à la sécurité d'Android, que Samsung a décidé de développer Samsung For Enterprise, puis Knox dès 2013. *"Nous souhaitions, en tant que fabricant, et grâce à nos relations avec Google, contribuer au renforcement de la sécurité mobile"*, précise Kevin Bambara. Depuis, à mesure des évolutions et innovations, Samsung Knox s'est imposé comme une solution indispensable. Et ce, sur l'ensemble du cycle de vie des terminaux : depuis l'acquisition en passant par la personnalisation et le déploiement, jusqu'au remplacement du smartphone.

"L'un des atouts de Samsung Knox, c'est aussi la progressivité de la réponse que nous apportons par rapport à la criticité des données et des usages des entreprises", précise Kevin Bambara. Parmi les éléments déterminants dans la stratégie de sécurisation des flottes portée par Knox, le chiffrement des données au niveau individuel, intégré sur la couche matérielle, ainsi que le cloisonnement pour étanchéifier les données utilisateurs, sont unanimement reconnus. En effet, la sécurisation native de Knox, reconnue et certifiée par l'ANSSI, mais aussi la stratégie de partenariats de Samsung avec des entreprises comme Pradeo ou Ercom (certifiée "Diffusion Restreinte" avec sa solution Cryptosmart), permettent de répondre à différents profils d'entreprises et enjeux. *"C'est la raison pour laquelle une trentaine de gouvernements dans le monde, pour lesquelles la sécurisation de la flotte mobile est une affaire d'état, ont opté pour Samsung Knox"*, conclut Kevin Bambara. Les certifications ANSSI et Gartner obtenues par Knox viennent d'ailleurs valider l'exigence de ses concepteurs, mais également la cohérence du réseau de partenaires certifiés, qui sont tous des experts reconnus de la sécurité mobile.

ON VOUS DIT TOUT SUR SAMSUNG KNOX !

Bien avant la crise sanitaire, les terminaux mobiles avaient envahi le quotidien des collaborateurs. Ce que cette période sans précédent a révélé en revanche, c'est la nécessité de pouvoir administrer et sécuriser ses équipements à distance, et en toutes circonstances ! C'est justement pour répondre à ces besoins stratégiques, que Samsung a conçu la suite de solutions professionelles Knox.

> *"Samsung Knox est une suite de solutions qui accompagnent un terminal dans tout son cycle de vie pour la sécurisation, la gestion et la productivité."*

résume Hamdi Abed, Channel Technical Account Manager chez Samsung Electronics France. Alors que les usages mobiles sont en pleine explosion, l'exposition du système d'information des entreprises aux malveillances et aux cyber-risques augmente considérablement. Il s'agit donc de tout mettre en œuvre pour que les terminaux mobiles ne créent pas de vulnérabilités dans les politiques de sécurité. *"Knox incarne en quelque sorte la philosophie de Samsung en ce qui concerne l'usage d'un terminal dans l'entreprise,* observe Adrien Pacgep, B2B Technical Project Manager Samsung Knox. *Cela passe principalement par la configuration, la sécurisation et l'optimisation par le biais d'une plateforme directement intégrée aux terminaux".* L'objectif pour l'entreprise ? Disposer d'une solution complète qui assure aux collaborateurs une expérience cohérente, homogène et parfaitement sécurisée sur l'ensemble des terminaux déployés. Pour y parvenir, Samsung Knox s'articule autour de différentes briques fonctionnelles.

Configurer, Enrôler, Manager, Sécuriser... La suite Knox a réponse à tout!

Dès le premier allumage d'un terminal, et jusqu'à son remplacement par un nouvel équipement, Samsung Knox est présent à toutes les étapes ! *"Le principe fondateur de notre démarche,* explique Hamdi Abed, *c'est que, quel que soit le besoin, il existe nécessairement un module dans l'écosystème Samsung Knox pour y répondre"*. Avec Knox Configure, les entreprises auront la possibilité de préparer l'intégration de nouveaux terminaux dans la flotte en créant différents profils uniques : paramètres, restrictions, applications et autres contenus. Puis, Knox Mobile Enrollment interviendra pour faciliter le déploiement des terminaux. En effet, lorsque les utilisateurs mettront leurs appareils en service et se connecteront au réseau, ils seront automatiquement inscrits auprès de l'EMM*. *"Knox Manage intervient dans un troisième temps,* précise Hamdi Abed, *afin de gérer les terminaux au quotidien et d'en contrôler l'usage par les collaborateurs pour affiner les stratégies"*. Parce que l'enjeu de la sécurisation de la flotte est plus déterminant que jamais, Samsung Knox Platform for Enterprise protège les données en les chiffrant non seulement lorsque l'appareil est éteint, mais également lorsqu'il est allumé et verrouillé et permet d'isoler des données professionnelles dans des applications et des conteneurs sécurisés. *"Enfin, Knox E-FOTA est la brique qui permet de rationaliser les mises à jour sur les terminaux. La garantie d'une maintenance optimale en minorant l'impact sur les utilisateurs finaux"*, précise Hamdi Abed.

Un tout-en-un au service de la sécurité et de la performance

"Samsung Knox Suite constitue la meilleure réponse aux idées préconçues sur les défauts de sécurité supposés de l'univers ouvert d'Android", analyse Adrien Pacgep. Si Android est par nature un écosystème fragmenté, Knox constitue un moyen d'uniformiser l'expérience de tous les modules. Sécurisation du démarrage d'un terminal, sécurisation des données, sécurisation des usages... la suite Samsung Knox est un ensemble d'API utilisables de façon modulaire, proposée par Samsung pour mieux gérer le terminal et le sécuriser. *"C'est la combinaison de ces savoir-faire et de ces techniques de protection qui font la philosophie de Samsung Knox"*, conclut Adrien Pacgep.

* Entreprise Mobile Management

SAMSUNG

Vous avez un projet mobilité pour votre entreprise ?

Pour nous contacter, cliquez ici

DoBusinesswithSamsung.com

KIT MAINS LIBRES RECOMMANDÉ

DAS Galaxy S20 : 0.279 W/kg , Galaxy S10 : 0.477 W/kg , Galaxy Note10 : 0,209 W/kg , Galaxy Note9 : 0,381 W/kg , Galaxy Tab Active2 : 0.539 W/kg

Le DAS (débit d'absorption spécifique) quantifie le niveau d'exposition maximal de l'utilisateur aux ondes électromagnétiques. La réglementation française impose que le le DAS ne dépasse pas 2W/Kg pour une utilisation à l'oreille et au niveau corps. L'utilisation d'un kit mains libres est recommandée.