Transformation technologique et évaluation du degré de préparation

BCG | verizon

Livre blanc

Deuxième opus de la série de livres blancs *Business as Unusual*

Auteurs

Sampath Sowmyanarayan
Jay Venkat
Michael Coden
Val Elbert

Introduction

Ce livre blanc est le deuxième d'une série consacrée au monde du travail de demain, notamment aux mesures que les entreprises doivent prendre pour intégrer le télétravail à leurs pratiques dans un monde où rien ne sera plus comme avant.

Si la pandémie de COVID-19 a bien montré une chose aux entreprises du monde entier, c'est que le télétravail n'est pas une question de choix, mais bel et bien un impératif absolu. L'avenir de nos environnements professionnels sera marqué par une quatrième vague d'adoption du télétravail à grande échelle, sous l'impulsion de technologies qui feront du distanciel un nouveau vecteur de compétitivité pour les entreprises.

Le premier article de notre série a étudié un à un les six impératifs d'efficacité du télétravail, à savoir :

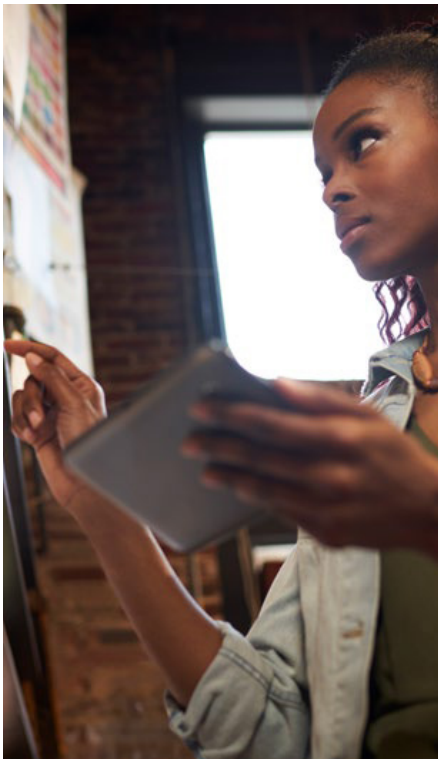
1. **Un réseau évolutif**
2. **Des applications compatibles avec le cloud**
3. **Une connectivité mobile robuste et sécurisée**
4. **Un suivi des performances de bout en bout**
5. **Une sécurité Zero Trust**
6. **Un modèle de support utilisateur résilient**

Bien entendu, le télétravail ne représente qu'un élément du monde du travail de demain. En outre, il est impossible de traiter ces six impératifs séparément : votre transformation technologique passe par une stratégie globale et holistique.

Dans notre premier article, nous nous demandions également si les entreprises étaient prêtes pour cette transformation technologique. Avec la crise sanitaire, leur stratégie de transformation n'a plus rien à voir avec ce qu'elle était il y a six mois, ni même il y a six semaines.

Les entreprises vont donc devoir relever des défis inédits, entre déploiements à grande échelle et adoption de technologies de nouvelle génération. Dès lors qu'ils sont soigneusement alignés et coordonnés, ces six impératifs constituent les piliers de la future croissance d'une entreprise.

Cet article a pour but d'éclairer les responsables technologiques sur les transformations à engager pour surfer sur la quatrième vague de télétravail annoncée. Nous y présenterons les grands impératifs à prendre en compte, les mesures tactiques et les solutions technologiques à disposition. Nous espérons ainsi aider toutes les entreprises à fixer un cap clair vers le monde du travail de demain.



Réinventer les plans de transformation technologique

Nous avons identifié un noyau dur de quatre étapes clés que les entreprises doivent suivre pour repenser leur plan de transformation technologique.

1. **Définir votre vision et vos objectifs de transformation.**
2. **Ériger la préparation de vos ressources humaines (effectifs et talents) au rang de priorité.**
3. **Créer des applications, des infrastructures IT et des plateformes data et digitales évolutives.**
4. **Intégrer la cybersécurité dès la conception.**

Quatre étapes clés pour repenser votre plan technologique

1. Définir votre vision et vos objectifs de transformation.

Les leçons à tirer de la pandémie de COVID-19 et du passage éclair au télétravail sont nombreuses. À l'heure où la quatrième vague d'adoption de ce modèle (telle que nous l'avons théorisée dans le premier article de notre série) se profile à l'horizon, les DSI doivent évaluer les performances de leur infrastructure IT pendant la crise et en tirer des conclusions. Quels éléments ont tenu le coup ? Lesquels ont déçu ? L'infrastructure IT s'est-elle montrée suffisamment résiliente ? L'efficacité, les processus et la productivité des effectifs ont-ils été impactés ? Sont-ils malgré tout parvenus à répondre efficacement aux besoins des clients ?

Au terme de cette réflexion, les DSI doivent d'abord définir la finalité ultime de la transformation de leur entreprise et leur modèle opérationnel cible à la lumière des six impératifs définis en introduction. Cette finalité doit être claire et, de par sa nature, procurer un avantage concurrentiel à l'entreprise. En règle générale, il est bon de s'appuyer sur des indicateurs spécifiques qui se traduiront par un ensemble d'actions rattachées à chaque pilier. Par exemple :

- Pour les réseaux, quel niveau d'évolutivité et de flexibilité nos schémas d'utilisation imposent-ils ? Quelle proportion de télétravailleurs prévoyons-nous (et dans quelles fonctions, à quels postes, dans quelles régions) ? Comment les besoins du réseau évolueront-ils à mesure que la courbe épidémique s'aplatit et que nous sortons de la crise, tandis qu'une partie de nos effectifs repasse en présentiel ?
- Pour la sécurité Zero Trust, à quel volume de menaces devrions-nous être confrontés chaque année, et avec quelle rapidité prévoyons-nous de les neutraliser après détection ?
- Pour le modèle de support utilisateur, l'expérience multicanal en ligne et la supply chain, quel nombre de fournisseurs envisager ? Dans quelle mesure souhaitons-nous nous diversifier ? Dans quelle mesure souhaitons-nous consolider nos systèmes ? Quelles sont les interdépendances de notre supply chain ?

Pour définir votre vision et vos objectifs de transformation, il est généralement conseillé de baser votre réflexion sur des indicateurs spécifiques.

Dans la même veine, et pour conclure ce point avec des exemples concrets, sur des centaines de projets, les études du Boston Consulting Group (BCG) soutiennent l'idée selon laquelle l'objectif des entreprises est de « développer des fonctions technologiques leaders qui les démarquent de la concurrence par l'introduction de nouvelles capacités numériques et par plus de simplicité (pour baisser les coûts) et de résilience ». (Reportez-vous au graphique à la page suivante.) Au vu de ces objectifs, les six piliers ont un rôle essentiel à jouer.

Source : "A World-Class Tech Function Is Digital, Simple and Resilient," BCG, 30 septembre 2019

Dans un autre article sur la gestion des cyber-risques liés au télétravail, le BCG détaille toutes les mesures de cybersécurité à appliquer aux effectifs en distanciel.

L'étape suivante consiste à définir la stratégie à adopter pour atteindre cet objectif. Cette stratégie doit tenir compte de votre situation du moment, qui est très certainement différente de celle d'avant-crise. De même, chaque entreprise aura un parc technologique très spécifique, en fonction de sa taille, de l'année de sa fondation et de sa présence géographique. Nous encourageons également les responsables techniques à définir clairement les besoins réseau de leur entreprise dans ce nouveau monde : utilisation plus flexible du réseau, hausse du nombre de télétravailleurs, commerce et engagement client numériques, supply chain numérique, différenciation par des hotspots mondiaux, etc. Ils doivent aussi imposer une transformation radicale, adaptée au caractère exceptionnel des circonstances, plutôt qu'une évolution progressive plus organique.

Il est alors essentiel de dresser un inventaire technologique complet (fonctions, architecture, environnement) pour avoir une image claire et complète de votre situation de départ.

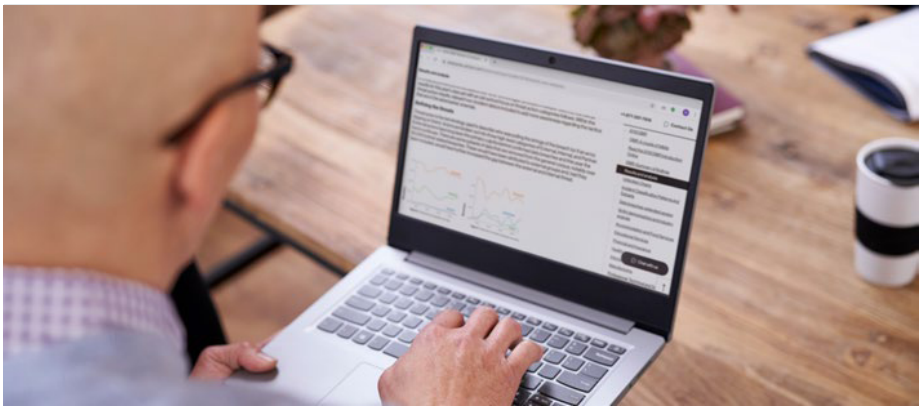
Identifiez vos ressources les plus stratégiques – vos fonctions et applications critiques, par exemple. Ainsi, vous pourrez créer des cas d'usage en phase avec vos objectifs métiers. Cela vous permettra également d'identifier les changements indispensables et les éléments à conserver. À partir de tout cela, vous pourrez façonner un plan complet qui capitalise sur vos ressources stratégiques d'aujourd'hui et de demain.

2. Ériger la préparation de vos ressources humaines (effectifs et talents) au rang de priorité.

Pour cette deuxième étape, assurez-vous que vous disposez des bonnes compétences pour concrétiser votre vision. Peut-être devrez-vous former vos collaborateurs existants dans des domaines comme l'intelligence artificielle (IA), le machine learning ou la cybersécurité. Peut-être devrez-vous recruter pour pouvoir remplir les six impératifs de votre transformation. Ou peut-être aurez-vous besoin de trouver un partenaire spécialisé pour vous accompagner dans cette démarche. Dans tous les cas, vous devez mettre en place la bonne équipe pour piloter votre transformation, sans quoi vous n'irez pas bien loin.

Vous devez mettre en place la bonne équipe pour piloter votre transformation, sans quoi vous n'irez pas bien loin.

Dès le départ, veillez également à ce que les équipes technologiques et les métiers soient parfaitement alignés et intégrés. Impossible de développer des technologies sans une boucle de feedback efficace pour faire remonter les retours d'expérience des utilisateurs. D'autant plus que, si une technologie n'est pas adaptée aux modes de travail de ces derniers, ils se rabattront sur une solution de rechange. Ici, les méthodologies Agile et le Human-Centered Design (HCD) ont toute leur place puisqu'ils facilitent les remontées du feedback client et y apportent des réponses rapides grâce à un juste équilibre entre alignement et autonomie. C'est un sujet que nous développerons dans le troisième article de notre série.



3. Créer des applications, des infrastructures IT et des plateformes data et digitales évolutives.

C'est à ce stade que la transformation se concrétise. Pour préparer votre entreprise à son avenir, vous devez avant tout vous doter d'une architecture IT modulaire, flexible et capable de relever les défis à venir. Vous devez donc simplifier votre environnement data et applicatif, puis miser sur les API et sur les microservices pour évoluer vers davantage de flexibilité. Pour cela, vous devez capitaliser sur l'infrastructure cloud privée, publique ou hybride qui vous permettra de monter en capacité le cas échéant. Vous devez également intégrer une cybersécurité renforcée à la conception et à l'implémentation de vos couches technologiques, de données et de plateformes.

4. Intégrer la cybersécurité dès le départ.

Intégrer la cybersécurité très en amont de votre transformation, c'est contrôler les coûts de développement et d'exploitation, réduire les délais d'implémentation et accélérer le retour sur investissement. D'après l'analyse de données client du BCG, cette approche peut en effet réduire les coûts de corrections et les délais de lancement de 62 % et 20 % respectivement. En outre, en instaurant un framework de cybersécurité commun à toutes les applications (sur site et multicloud), vous pouvez réduire vos coûts d'exploitation de 40 %.

Un framework de cybersécurité commun à toutes les applications peut réduire les coûts d'exploitation de 40 %.

Peu d'entreprises prennent le temps de suivre minutieusement ces quatre étapes. D'où un taux anormalement élevé de projets de transformation qui soient dépassent les budgets, soient échouent. Lorsque vous ne prenez pas la peine de dresser un état des lieux de votre situation, de vous doter des compétences dont vous aurez besoin et d'intégrer la flexibilité dès le départ, vous risquez également de rencontrer de graves problèmes plus tard.

Quoi qu'il en soit, pour passer de la théorie à la pratique, vous devrez investir dans les technologies et dans le développement des compétences de vos équipes. C'est pourquoi il est essentiel de planifier en amont ces investissements et les retours attendus. Mais cela passe par une vision à long terme. Il est très facile de privilégier les économies à court terme au détriment des avantages à long terme d'une implémentation de tous ces piliers. Les meilleurs plans de transformation sont ceux qui parviennent à trouver le juste équilibre : ils concilient ces différents impératifs dans un ordre économiquement réfléchi.

Piliers techniques de la transformation

Étudions maintenant en détail les six impératifs listés en introduction.

01 Un réseau évolutif

Pour ce premier pilier, la première chose à faire consiste à dresser un état des lieux de tout l'environnement. Rappelons qu'un bilan de l'architecture de base et des fonctions réseau communes constitue un point de départ essentiel au développement d'un plan de transformation technologique. Vous devez ensuite dessiner les contours de futurs modes opérationnels potentiels par le biais d'exercices de préparation à deux ou trois scénarios majeurs (pandémie, catastrophe naturelle, perturbation de la supply chain, etc.). Ce travail préparatoire vous aidera à établir une feuille de route architecturale en phase avec vos objectifs métiers.

Les éléments les plus importants d'un réseau évolutif restent sans aucun doute la flexibilité et l'évolutivité. C'est là que le SDN entre en jeu.

Toutefois, les éléments les plus importants de ce pilier restent sans aucun doute la flexibilité et l'évolutivité. Pour rester dans la course à la compétitivité sur des marchés mondiaux très volatiles (pendant et après la pandémie), toutes les entreprises ont besoin d'un réseau capable de répondre en temps réel aux besoins changeants de leurs utilisateurs et de leurs applications (hausse de la bande passante en période de soldes, nouvelles demandes de connexions VPN ou d'accès cloud pour les basculements en télétravail, etc.). C'est là que le SDN (Software-Defined-Networking) entre en jeu.

Depuis toujours, les entreprises ont dû recourir à différents équipements matériels pour répondre à des besoins réseaux spécifiques (routeurs, commutateurs, pare-feu, équilibreurs de charge, etc.). Grâce au SDN, toutes ces fonctionnalités s'exécutent désormais par logiciel en mode virtuel. Cette technologie rend le réseau plus flexible, agile et élastique, dans la mesure où les logiciels permettent d'augmenter les capacités ou d'introduire de nouvelles fonctionnalités. Le SDN favorise l'innovation bien mieux que les réseaux statiques. Si SDN ne rime pas toujours avec évolutivité, l'inverse est inconcevable : qui dit évolutivité dit toujours SDN. Un réseau SDN évolutif comporte quatre grandes caractéristiques :

Reconnaissance des applications/utilisateurs

Dans n'importe quelle organisation, tous les utilisateurs et toutes les applications n'ont pas la même importance. D'où l'intérêt de la segmentation. Par exemple, un système ERP a un niveau de criticité plus élevé que la navigation web. Dans la même veine, certains utilisateurs sont plus importants que

d'autres (praticiens dans l'univers de la télémédecine, traders dans la finance, etc.). Le SD-WAN (WAN logiciel), une sous-catégorie des réseaux SDN, est capable de reconnaître les applications et utilisateurs, ce qui permet aux entreprises de les classer par ordre de priorité. Pour aller encore plus loin, il est possible d'associer le SD-WAN à des fonctions de visibilité réseau avancées (abordées dans le détail ci-dessous).

Virtualisation des fonctions (NFV) réseau pour des montées en charge rapides

Déployés dans le cadre de la virtualisation des fonctions réseau, les VPN adaptent leurs capacités bien plus facilement et rapidement (quelques heures ou jours au lieu de plusieurs semaines) que les réseaux matériels. Ainsi, nombre de nos clients ont considérablement augmenté les débits de leurs VPN afin de faciliter le passage au télétravail. Par exemple, pour absorber la hausse soudaine des accès en distanciel, deux entreprises européennes sont passées en NFV pour atteindre des débits de connexions VPN supérieurs à 1 Gbit/s à travers plusieurs nœuds réseau.

De son côté, une entreprise du tertiaire basée en Inde a implémenté un VPN SDN dans l'urgence pour prendre en charge ses utilisateurs travaillant depuis chez eux pour la première fois. S'il est vrai que la NFV a eu du mal à s'imposer ces dernières années, on devrait assister à une accélération de son adoption. D'après le cabinet Gartner, « 39 % des entreprises citent le risque fournisseur et technologique comme un obstacle majeur à une adoption plus large des services NFV. Les principaux fournisseurs de services réseau s'efforcent d'élargir leur offre de plateformes matérielles et de fonctions logicielles tout en maintenant la qualité et en réduisant la complexité. »[1]

Orchestration par API

Les API améliorent la visibilité sur la bande passante et le routage du trafic à travers tous les réseaux publics et privés. Les outils de visibilité, que nous aborderons plus tard dans ce document, détecteront tout problème ou anomalie d'infrastructure (lié à un pic de demande client ou au passage rapide au télétravail, par exemple), puis transmettront ces informations à des workflows prédéfinis chargés d'invoquer les appels d'API aux éléments réseau (NFV, réseaux Internet et MPLS traditionnels, 5G, etc.). Ainsi, votre entreprise peut monter en capacité afin de prévenir tout problème, le tout sans intervention humaine.

Par exemple, une grande enseigne internationale basée aux États-Unis a pu booster ses connexions réseau dans l'heure. Cette montée en charge aurait pris plusieurs jours sans les API. De son côté, une entreprise européenne de leasing a profité des API pour mettre à jour ses politiques et donner la priorité à ses applications critiques en période de saturation réseau.

Accès flexible au cloud

Pour un réseau vraiment évolutif, le dernier élément à mettre en place concerne les interconnexions cloud, à savoir des réseaux publics et privés vers les fournisseurs SaaS et le cloud hyperscale.

Souvent, les applications et composants applicatifs continueront d'être hébergés dans différents clouds, mais il doit être possible d'y accéder rapidement et facilement. Les fournisseurs cloud et SaaS doivent donc être considérés comme une extension du réseau, avec des architectures d'interconnexion cloud capables d'ajuster rapidement les accès et la bande passante, des modèles de facturation à l'usage et un accès défini par logiciel à des data centers en colocation, le tout sans aucune installation de nouvelles connexions physiques.

C'est ainsi qu'une holding latino-américaine a pu compter sur son accès SDN aux géants du cloud pour booster la connectivité à Microsoft® Azure® pour ses télétravailleurs.

Les fournisseurs cloud remplacent généralement leur matériel tous les deux ans, tandis que la plupart des grandes entreprises procèdent à un tel renouvellement tous les quatre à sept ans, ce qui se traduit par une hausse de 20 % des performances.

02 Des applications compatibles cloud

Là encore, la première chose à faire consiste à dresser l'inventaire des applications existantes et de celles pouvant d'ores et déjà migrer vers le cloud. Et comme pour tous les inventaires, cet exercice doit être répété fréquemment. D'après un rapport du BCG, « les fournisseurs cloud remplacent généralement leur matériel tous les deux ans, tandis que la plupart des grandes entreprises procèdent à un tel renouvellement tous les quatre à sept ans, ce qui se traduit par une hausse de 20 % des performances. Ils doivent cette hausse à la loi de Moore, mais aussi à l'accélération de l'accès aux données et à de meilleurs systèmes d'exploitation et logiciels de virtualisation. »[2] Pour les organisations de plus petite taille, la transition vers le cloud est plus facile puisqu'elles s'appuient déjà souvent sur un plus grand nombre d'applications SaaS.

Une fois l'inventaire réalisé, il s'agit de migrer les applications compatibles cloud (et les workflows connexes), puis d'établir une stratégie « cloud-first » centrée sur la sécurité pour les futures migrations d'applications. D'après le BCG, « les grandes entreprises qui réussissent leur passage au cloud peuvent enregistrer une amélioration de 25 % à 50 % des performances de leurs services IT ».[2]

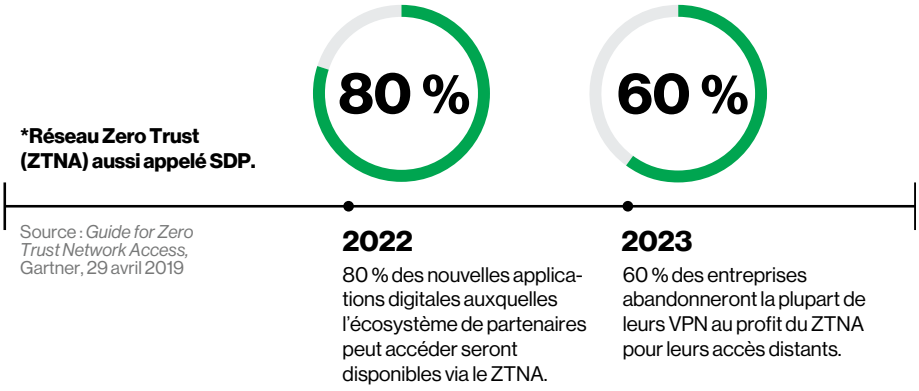
1 *Market Trends: SD-WAN and NFV for Enterprise Network Services*, Gartner, 30 janvier 2020
2 https://www.bcg.com/publications/2019/enterprise-applications-cloud-ready-prime-time.aspx

Par la suite, vous devez définir votre stratégie de collaboration et choisir une plateforme pour vos communications internes – et potentiellement pour interagir avec vos partenaires, vos fournisseurs et vos clients. Là encore, réfléchissez aux politiques et procédures à mettre en place pour respecter les éventuelles réglementations sectorielles en vigueur. Bien définir cette stratégie de collaboration en amont, c'est sélectionner une solution de communication unifiée et adaptée à vos propres besoins. Certaines entreprises utilisent énormément la vidéo, tandis que d'autres recourent davantage au chat.

Lorsque vous migrez vos applications dans le cloud, il est important d'envisager des solutions logicielles de protection de votre périmètre réseau. Capables de sécuriser à la fois des infrastructures en pleine mutation et la surface d'attaque applicative, ces solutions commencent à gagner du terrain (cf. figure ci-dessous).

Ensuite, vous devez surveiller ces ressources à travers vos réseaux et serveurs cloud, surtout en cas de déploiements hybrides. Cela pourra passer par un contrôle d'accès des utilisateurs et des développeurs aux applications cloud, ou encore un suivi des changements et mises à jour. Vous devez également pouvoir évaluer en continu votre sécurité cloud à la lumière des bonnes pratiques sectorielles (intégration des logs, tests d'intrusion, gestion des vulnérabilités, etc.). Enfin, réfléchissez à l'accès au cloud (y compris l'accès des réseaux privés aux principales ressources cloud) et à son système de sauvegarde, ainsi qu'aux fonctionnalités de contrôle et de visibilité sur les multiples nœuds du cloud.

Solutions Software Defined Perimeter (SDP)*



***Réseau Zero Trust (ZTNA) aussi appelé SDP.**

Source : *Guide for Zero Trust Network Access*, Gartner, 29 avril 2019

Pour des connexions mobiles renforcées et sécurisées, vous ne devez surtout pas négliger la qualité des connexions physiques. Par conséquent, envisagez plusieurs options pour obtenir le bon niveau de performance.

03 Des connexions mobiles renforcées et sécurisées

Pour ce pilier, il est primordial de déployer des connexions fiables et sécurisées. Ici, vous ne devez surtout pas négliger la qualité des connexions physiques. Par conséquent, envisagez plusieurs options pour obtenir le bon niveau de performance. Par exemple, un client Verizon (un établissement financier international) a récemment déployé des hotspots LTE pour mieux couvrir les zones où les connexions haut débit grand public ne répondaient pas aux attentes.

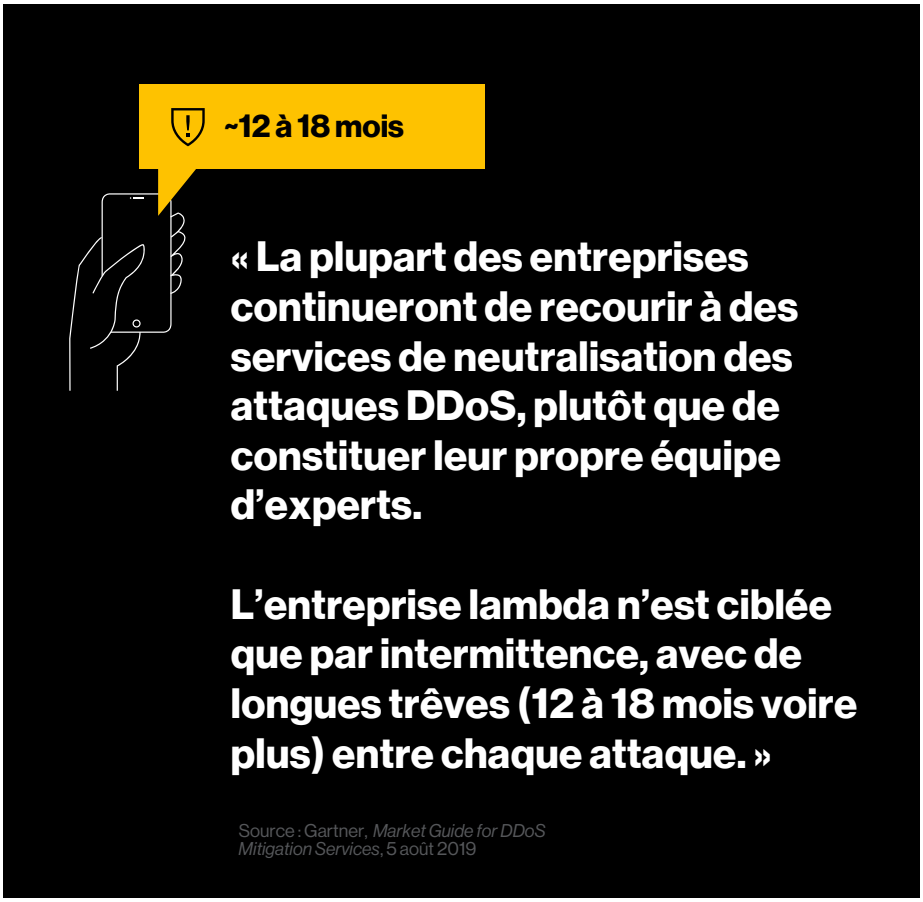
Les VPN constituent un autre élément clé de ce pilier. Pour améliorer leurs performances, pensez aux services de passerelle sans fil privés. Toutefois, la sécurité ne doit pas passer au second plan. Elle doit être systématiquement intégrée en amont. Au-delà de la simple protection antivirus, il s'agit de lutter contre les vulnérabilités zero-day et, dans la mesure du possible, d'exploiter l'IA et la Threat Intelligence pour prédire les éventuelles compromissions de données.

Par exemple, une compagnie américaine d'assurances et de placements du Fortune 500 a déployé une solution intégrée de prévention des menaces qui allie le blocage par IA des infections par malware à une haute efficacité et un faible impact sur les systèmes pour prévenir les attaques zero-day. La solution s'exécute là où la plupart des attaques se produisent (sur les terminaux) pour une meilleure efficacité, une neutralisation rapide et des perturbations minimes.

Il va sans dire que chaque équipement de connectivité filaire et sans fil doit pouvoir être déployé rapidement, mais sous contrôle. Vous devez également pouvoir surveiller les déploiements d'applications mobiles non autorisées. Par exemple, une société d'investissement américaine présente dans le monde entier a récemment déployé plus de 7 000 terminaux pour ses télétravailleurs de façon à gérer le trafic par priorité et à obtenir toute la visibilité nécessaire au respect des obligations règlementaires. Enfin, vous devez gérer minutieusement les politiques et l'accès aux sites web publics via des services de breakout Internet régionaux.

L'accès distant dynamique et adaptable, la gestion des appareils mobiles et la sécurité des terminaux figurent parmi les solutions à envisager pour renforcer et sécuriser vos connexions mobiles. Ces solutions doivent être complétées par des services de protection du DNS pour le blocage des malwares sur le réseau, par des solutions de breakout et de passerelle Internet pour le contrôle des politiques et l'amélioration globale des performances, et par des systèmes anti-DDoS pour permettre à une population croissante de télétravailleurs d'accéder aux ressources d'entreprise en toute sécurité.

Gardez également à l'esprit le fait qu'en matière de sécurité, l'humain constitue souvent le maillon faible de votre entreprise. Vous devez donc former vos salariés et les sensibiliser en permanence aux gestes simples à adopter contre le phishing, les malwares et l'ingénierie sociale, sans oublier l'intégration des flux de Threat Intelligence au système de filtrage des e-mails.



Le *Rapport d'enquête Verizon sur les compromissions de données* (DBIR) offre une excellente source d'informations sur la sécurité et les menaces en présence. Enfin, n'oubliez pas que le meilleur moyen de protéger votre réseau reste de poser des bases saines. D'où l'importance capitale de bien appliquer les correctifs et mises à jour en temps et en heure.

Gardez également à l'esprit le fait qu'en matière de sécurité, l'humain constitue souvent le maillon faible de votre entreprise. Vous devez donc former vos salariés et les sensibiliser en permanence aux gestes simples à adopter contre le phishing, les malwares et l'ingénierie sociale.

04 Suivi des performances de bout en bout

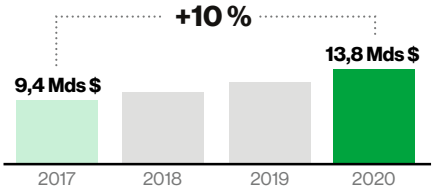
Pour ce quatrième pilier, la première chose à faire consiste là encore à dresser un inventaire de façon à bien cerner les flux de données qui transitent sur votre réseau. Ensuite, vous devez définir le fonctionnement de ce dernier en termes de visibilité, d'analyse et d'exécution. Nous nous appuyons sur l'enquête du BCG auprès d'experts du secteur pour couvrir les neuf principaux cas d'usage rattachés à ces trois volets (cf. figure à la page suivante).

L'adoption dépendra de la chaîne de valeur des opérations IT.

	Principaux cas d'usage	IAOps utilisée actuellement (%)	IAOps utilisée actuellement (%)
Visibilité	Détection des anomalies	11	42
Analyse	Réduction des faux positifs	9	42
	Tri et corrélation des alertes	10	10
	Analyse d'impact du service	5	35
	Analyse des causes racines	6	33
	Prévisions	9	38
	Prédiction des incidents	9	38
Exécution	Recommandations pour la remédiation	7	32
	Remédiation automatisée	3	21

IAOps : IA intégrée aux opérations
Source : Entretiens avec plus de 25 experts du secteur.
Enquête DSI (N=112), analyse du BCG, août 2019

Analyse du BCG : taux de croissance annuel composé sur trois ans



La valeur du marché de l'IAOps devrait passer de 9,4 milliards de dollars en 2017 à 13,8 milliards de dollars en 2021, soit une croissance annuelle composée de 10 %.

Le segment des orchestrateurs IAOps – des plateformes conçues pour orchestrer les analyses et les actions en fonction des données de logs de différentes solutions de monitoring – devrait croître de 25 % sur la même période.

Source : Analyse du BCG, août 2019

Dans l'ensemble, le but est de constituer un référentiel de données fiable pour comprendre comment renforcer les différentes portions du réseau, en y intégrant l'analyse prédictive pour anticiper et prévenir les pannes et anomalies et en automatisant certaines actions aux niveaux des utilisateurs, transactions ou applications.

À l'heure où les flux de données des entreprises passent d'une configuration essentiellement centrée sur les bureaux à des accès en distanciel, les DSI doivent pouvoir ponctionner des données directement à partir du réseau afin d'identifier et de bloquer rapidement les comportements anormaux. Par exemple, dans une grande entreprise, Verizon a constaté une explosion (plus de 200 %) du trafic UDP (User Datagram Protocol) par rapport au trafic TCP (Transmission Control Protocol) plus traditionnel. Après inspection approfondie des ports, ce trafic se rapportait presque exclusivement aux VPN des télétravailleurs.

Dans ce cas de figure, le changement de protocole était prévisible, mais un haut niveau de visibilité s'avère nécessaire pour confirmer ce type de prévisions.

Toutefois, le mieux reste encore de piloter les opérations IT par intelligence artificielle (on parle de solutions IAOps) pour transformer les Big Data en informations exploitables, capables de simplifier et d'améliorer l'orchestration et la gestion réseau. Les études BCG montrent que le marché des solutions IAOps est en plein essor.

Pour maintenir les performances, le mieux reste encore de piloter les opérations IT par intelligence artificielle (on parle de solutions IAOps) pour transformer les Big Data en informations exploitables, capables de simplifier et d'améliorer l'orchestration et la gestion réseau.

Les équipes informatiques accordent une importance particulière au monitoring. Du côté des métiers, tout est question de productivité et de moral des troupes. Pour tout cela, la visibilité s'avère indispensable. Au final, ce qui compte vraiment, c'est l'expérience des collaborateurs sur les applications critiques. L'objectif est donc d'identifier les causes des pertes de productivité et d'y remédier, même lorsque l'Internet ou le réseau qui sous-tendent vos applications ne vous appartiennent pas et que vous n'avez que peu de marge de manœuvre pour paramétrer les plateformes SaaS qui exécutent vos applications. Votre supply chain numérique est un mélange de ressources publiques, privées, personnelles, professionnelles et autres. Il est donc primordial de bien cerner l'expérience utilisateur (tant interne qu'externe) de bout en bout.

C'est pourquoi le BCG et le NIST (National Institute of Standards and Technology) ont développé conjointement un certain nombre de pratiques essentielles pour les supply chains numériques, ainsi qu'un outil logiciel open-source cartographiant les interdépendances de la supply chain pour vous faciliter sa gestion.

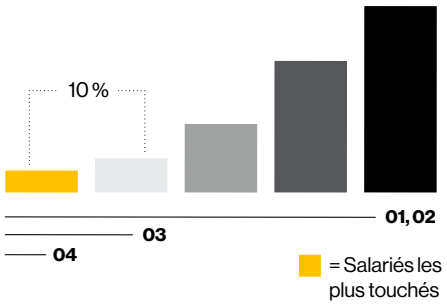
Les profils de visibilité sont paramétrés de façon à afficher des relevés, seuils et timings, et à signaler les différents états du service (en cours d'exécution, interrompu ou dégradé), tout en informant sur l'impact associé. L'analyse de l'écosystème numérique de votre entreprise à la lumière des scores d'expérience/numériques (similaires aux scores MOS [Mean Opinion Score] pour la qualité de la téléphonie), des résultats métiers et de l'expérience humaine permet de mieux corréler et contextualiser les données. À la clé : des délais de réparation plus courts et la possibilité de déployer une automatisation pilotée par IAOps.

Parmi les solutions à envisager figurent le monitoring synthétique des transactions, de l'expérience utilisateur basée sur les rôles et des processus métiers, sans oublier l'automatisation intelligente des workflows.

Prenons l'exemple d'un outil de visibilité que Verizon a déployé en interne et chez des clients. Le partenaire technologique de Verizon, Actual Experience, propose un outil de mesure synthétique des écosystèmes numériques. Il utilise ensuite des algorithmes avancés « d'expérience humaine » et des techniques de corrélation pour identifier rapidement la cause de la perte de productivité (Wi-Fi du domicile, FAI local, infrastructure d'entreprise ou fournisseur de service cloud). Le graphique ci-dessus illustre certaines des informations exploitables tirées de ce type d'outils pour une business unit de Verizon Business Group. À mesure que les entreprises conduiront et étendront des tests de visibilité de ce genre, les indicateurs de productivité ainsi obtenus aideront à définir des portions prioritaires de leur supply chain pour optimiser l'utilisation de leurs ressources. Là encore, les résultats pourront différer d'une division ou d'une application à une autre. Mais c'est tout l'intérêt de la granularité des données, qui permet d'approfondir l'analyse pour en dégager des cas particuliers.

Exemple sélectionné : une division du groupe Verizon Business et près de 40 implantations

Principaux résultats



01
4 min
Temps perdu par jour et par salarié en moyenne

02
Aucune perte
Temps perdu par jour 30 % des salariés

03
>15 min
Temps perdu par jour 10 % des salariés

04
31 min
Temps perdu par jour Salariés les plus touchés

Causes racines

Wi-Fi **19 %**

FAI **70 %**

VPN **79 %**

Cloud **11 %**

05 Une sécurité Zero Trust

D'après la définition de la NIST américaine, « [la sécurité] Zero trust [se concentre] sur la protection des ressources, et non celle des segments réseau, dans la mesure où l'emplacement d'une ressource sur le réseau ne représente plus le principal facteur de son niveau de sécurité. » Pour ce pilier, vous devez d'abord identifier les applications et flux de données les plus essentiels à votre entreprise, sans lesquels vous ne pourriez pas opérer. Il pourra s'agir de données, de ressources virtuelles ou de matériels physiques comme des équipements industriels ou des infrastructures de transport d'énergie.

À cet égard, les vastes réseaux mondiaux de données et de communication vocale de Verizon lui donnent une excellente visibilité sur l'impact du COVID-19. De l'ingénierie sociale sur le réseau voix à l'évolution des tendances de communication, en passant par les menaces associées et les vulnérabilités nées de la généralisation rapide du télétravail, Verizon bénéficie d'un panorama complet. Une étude du BCG montre que les groupes d'attaquants étatiques ciblent les familles de dirigeants d'entreprise, sachant que tous leurs membres utilisent le même réseau non sécurisé à domicile. Une fois l'appareil d'un membre de la famille compromis, les attaquants tentent d'accéder à l'ordinateur portable du dirigeant et d'infiltrer les systèmes de son entreprise.

Habituellement, les arnaques basées sur l'ingénierie sociale sont motivées par l'appât du gain (numéros de carte bancaire, informations de compte en banque, etc.) ou la collecte d'identifiants qui serviront à commettre des fraudes ou à compromettre la sécurité des systèmes critiques d'une entreprise. Verizon utilisent ses propres outils d'intelligence réseau pour capturer, catégoriser et journaliser des centaines de milliers de spams et d'appels de bots par jour. Ainsi, nous avons identifié nombre d'arnaques en rapport avec le COVID-19 : kits de test gratuits, aide à l'accès aux fonds de relance, etc. Verizon travaille avec les pouvoirs publics et d'autres partenaires pour identifier et neutraliser les auteurs de ces arnaques à mesure qu'elles émergent et évoluent.

Ces menaces s'avèrent d'autant plus dangereuses qu'elles peuvent compromettre le périmètre de sécurité des entreprises qui s'étend désormais jusqu'au domicile des collaborateurs. Côté hackers, on constate une concentration des attaques sur les appareils intelligents que les utilisateurs considèrent habituellement comme sûrs. À terme, les DSI et les RSSI vont devoir intégrer des outils adaptés à leur stratégie de sécurité et conclure de nouveaux partenariats afin de tenir compte de ce type d'attaques.

Pour commencer, réfléchissez à la création de réseaux microsegmentés, protégés par des pare-feu de dernière génération, pour autoriser l'accès aux applications plutôt qu'aux réseaux eux-mêmes. Ces réseaux devraient suivre la stratégie Zero Trust énoncée dans la publication spéciale 800-207 du NIST. En clair, isolez les serveurs et déployez l'authentification multifacteur et le chiffrement de bout en bout pour lutter contre le vol d'identifiants. Veillez également à couvrir tant les applications et les données de vos data centers que celles du cloud.

Vous devez ensuite envisager de renforcer la sécurité de vos flux de données d'applications et d'authentification en séparant le chemin de données de son unité de contrôle. N'oubliez pas non plus la question des privilèges d'accès aux applications. La solution : des jump hosts qui établissent une zone de sécurité séparée pour l'accès et la gestion des équipements. Vous devez également vous pencher sur les besoins réels de partage et d'accès aux applications de vos partenaires et développer des modèles destinés à étendre la chaîne de confiance à des ressources comme votre supply chain, vos appareils IoT et vos systèmes de comptabilisation des transactions. Peut-être plus important encore, vous devez créer un plan complet de réponse à incident, avec implémentation de fonctionnalités dynamiques et actualisées de détection et d'analyse des menaces. En étroite collaboration avec le Massachusetts Institute of Technology (MIT) et le Forum économique mondial, le BCG a développé des exercices de simulation uniques, destinés à identifier et à combler les lacunes des plans de réponse à incident et de continuité d'activité.

Autre élément clé du modèle de sécurité Zero Trust : les solutions de protection SDP. Ces solutions érigent un « rempart virtuel » autour de vos applications et de vos équipements pour mieux les protéger contre les menaces potentielles. Que vous utilisiez des applications SaaS ou vos propres applications hébergées dans le cloud, elles rapprochent ces applications des utilisateurs pour améliorer leur expérience, avec en prime des services de breakout Internet et un accès direct au cloud. Les enclaves IaaS sécurisées constituent elles aussi une bonne option, surtout dans un contexte de croissance rapide de ce type d'infrastructure.

Dans de nombreux secteurs d'activité, nous avons vu de nombreuses entreprises déployer des solutions SDP. En voici trois exemples :

Exemple 1

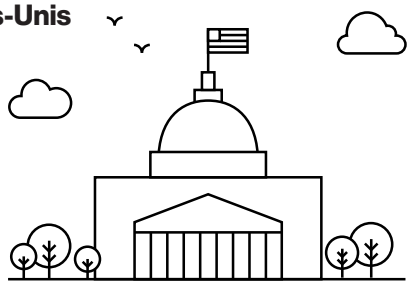
Accès sécurisé à plusieurs clouds pour un établissement financier aux États-Unis

Contexte et enjeux

- Tenté par l'agilité du cloud mais interdit par les lois bancaires fédérales
- A d'abord envisagé le cloud Amazon Web Services™, mais s'est vu proposé un accès gratuit à des serveurs Microsoft Azure
- L'enjeu est d'identifier une solution qui permet d'accéder à de multiples clouds en toute sécurité

Solutions

- Services partagés, de tests et de production configurés dans les deux clouds avec un accès isolé par le SDP
- Aide au respect des exigences du Federal Financial Institutions Examination Council (FFIEC), et accès rapide et simultané à AWS et à Azure via des passerelles sur chaque cloud



Exemple 2

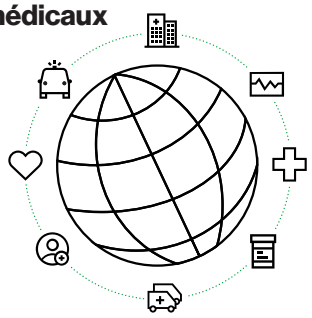
Configuration des accès privilégiés pour un fournisseur mondial d'équipements médicaux

Contexte et enjeux

- En quête d'un environnement DevOps capable d'octroyer des fonctions d'administration serveur à ses développeurs
- Une politique existante interdit les accès par SSH (Secure Shell) côté utilisateur du réseau
- Développeurs dispersés à travers le monde, ce qui complique la donne

Solutions

- Solution SDP pour permettre aux développeurs d'accéder aux serveurs par tous les ports nécessaires tout en en bloquant l'accès aux utilisateurs et aux terminaux non autorisés
- Maintien de la politique d'accès par SSH, mais accès des développeurs aux serveurs



Exemple 3

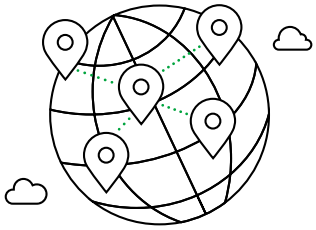
Contrôle d'accès pour un fabricant mondial d'équipements de télécommunications

Contexte et enjeux

- Le développement produit repose sur des centaines d'ingénieurs logiciels à travers le monde, différents types de collaborateurs (temps plein, indépendants) et des modes de travail disparates (sur site, à distance, télétravail)
- Besoin d'une solution qui protège le référentiel logiciel contre les attaques tout en fournissant un accès mondial aux ingénieurs autorisés

Solutions

- Solution SDP adossée à l'authentification multifacteur (MFA) intégrale, à l'isolement des serveurs et à des moyens de lutte contre les attaques par interception (MITM)



Parmi les solutions complémentaires au modèle de sécurité Zero Trust, citons le déploiement de solutions de détection et de réponse réseau pour des services d'inspection avancés, ou encore les solutions managées de détection et de réponse qui aident à réduire les délais entre une compromission et sa réalisation. N'oubliez pas non plus de tester vos solutions dans le cadre d'exercices de simulation afin d'évaluer votre niveau de préparation.

06 Un modèle de support utilisateur résilient

Si peu d'entreprises considèrent un modèle de support utilisateur résilient comme l'un des piliers de leur croissance, ce modèle s'avère pourtant crucial pour leur transformation. Les utilisateurs n'auront plus nécessairement accès à un support technique sur site ou à des services internes du même type. Vous devez donc vous assurer que vos salariés, vos partenaires et vos clients ont accès aux bonnes technologies, dans la forme la mieux adaptée qui soit. Pour favoriser l'appropriation des nouvelles technologies par les utilisateurs, créez une stratégie de déploiement claire. Veillez également à mettre en place des moyens de communication efficaces pour les accompagner, tant dans le cadre des déploiements de nouvelles technologies que des processus métiers quotidiens. Par exemple, Verizon a réassigné 700 salariés de ses magasins vers son service de télévente et son service client. Pour cela, ses protocoles, ses formations et ses outils se sont avérés essentiels. C'est pourquoi ces éléments doivent être intégrés à la planification globale de l'entreprise.

Parmi les indispensables figurent les fonctions de chat, les tutoriels vidéo et livres blancs, les communiqués réguliers et le self-service digital (pour autonomiser les utilisateurs et permettre à l'équipe de support de se concentrer sur les problèmes les plus graves). Il est également important d'entretenir un dialogue permanent via une page web, la collaboration vidéo, les appels audio, des sessions d'accompagnement en direct ou, pourquoi pas, une bonne vieille newsletter. Plus essentiel encore, vous devez créer un système de support flexible, capable de s'adapter à l'évolution des besoins des utilisateurs.

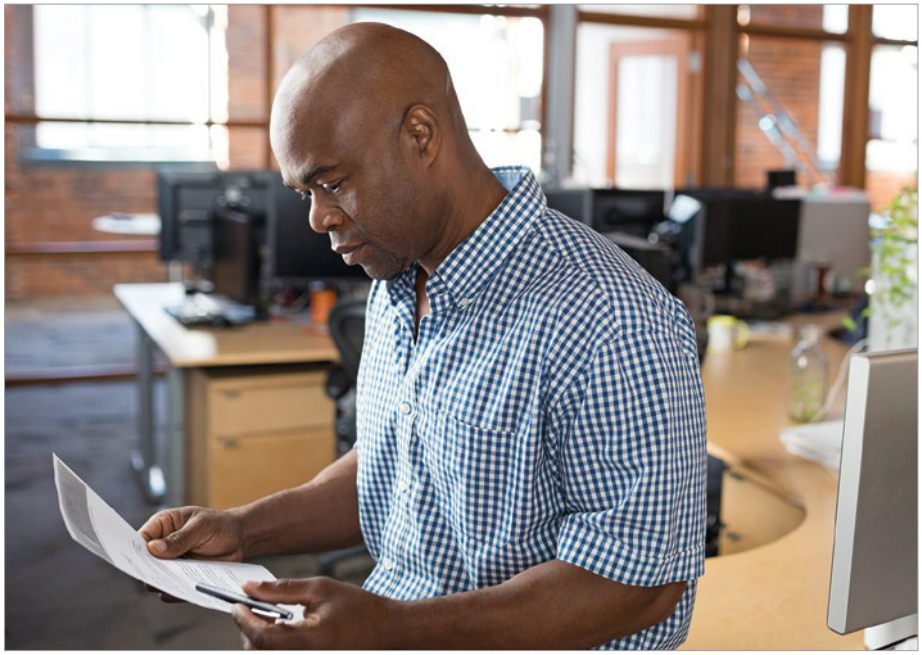
Enfin, les entreprises doivent se pencher sur les technologies critiques de leur supply chain numérique et articuler un plan de continuité d'activité associé. Si tout un business model repose sur les tablettes et que toute la production est interrompue par une catastrophe naturelle, une pandémie ou autre, qu'adviendra-t-il de l'entreprise ? N'importe quelle organisation gagnerait à organiser des exercices de simulation et à identifier ses lacunes.

N'importe quelle organisation gagnerait à organiser des exercices de simulation et à identifier ses lacunes.

À vous de jouer.

Nous venons d'exposer les grandes lignes du plan de transformation technologique et de la checklist que les entreprises doivent suivre pour poser les bases techniques nécessaires à la généralisation du télétravail. Cette manne d'informations dresse un tableau complet des mesures à prendre dès maintenant pour pérenniser votre activité.

Il est toutefois essentiel de procéder par étape. Vous devez d'abord établir une stratégie d'entreprise claire avant de parcourir la checklist pour vérifier si vous disposez des éléments indispensables pour entamer (ou poursuivre) votre transformation. Une chose est sûre : en suivant les étapes décrites dans ce livre blanc, vous aurez une idée assez précise de la capacité de votre entreprise à surfer, ou non, sur la quatrième vague d'adoption du télétravail dans un monde où plus rien ne sera comme avant.



Notre prochain volet examinera les tendances bien particulières qui sous-tendront le monde du travail de demain, ainsi que leurs répercussions sur le facteur humain (cf. plan de transformation technologique des pages précédentes) et l'attitude indispensable des dirigeants pour mener leurs troupes en distanciel dans le « monde d'après » – un autre sujet auquel nous faisions allusion dans le premier article.

Auteurs

Sampath Sowmyanarayan, Président, Global Enterprise, Verizon Business

Jay Venkat, Directeur général et associé principal, Responsable North America Technology Advantage Practice Area, Boston Consulting Group

Michael Coden, CISSP, Directeur général, Responsable Cybersecurity Practice, Boston Consulting Group Platinion

Val Elbert, Directeur général et associé, Boston Consulting Group