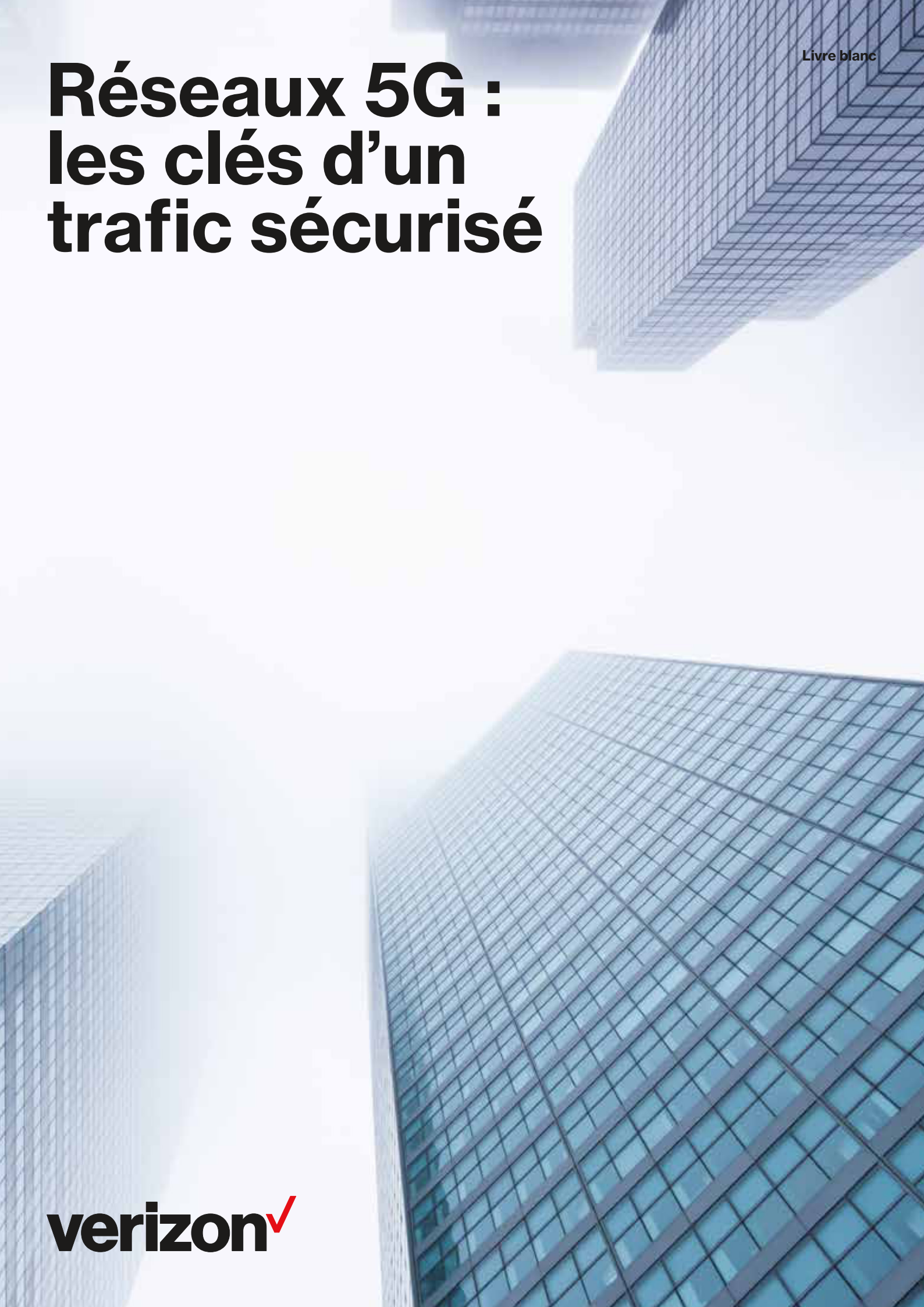
Livre blanc

Réseaux 5G : les clés d'un trafic sécurisé



verizon

Alors que le nombre d'appareils connectés devrait passer de 31 à 75 milliards d'ici à 2025[1], le formidable essor de l'IoT fait exploser les volumes de données dans les entreprises. Pour les équipes IT, le défi est de taille : déployer des réseaux plus rapides et capables de prendre en charge une plus forte densité d'appareils, tout en assurant la sécurité et la bonne gouvernance des données. Selon le rapport Verizon DBIR 2020, près de 90 % des compromissions sont guidées par des motivations financières[2]. Compte tenu de l'énorme volumétrie de données propriétaires créées, transférées et stockées, l'adoption de la 5G devrait impacter la sécurité globale de toutes les entreprises.

Après un tour d'horizon des menaces en présence, ce livre blanc vous invite à faire le point sur les opportunités et les risques des nouveaux cas d'usage de la 5G.

Des menaces en évolution

Un rapide coup d'œil du paysage actuel de la sécurité nous donne une idée des menaces qui accompagneront l'émergence de la 5G. Sur ce point, le rapport Verizon DBIR 2020 est édifiant : 45 % des compromissions sont le fait direct de hackers, tandis que 22 % s'expliquent par des erreurs diverses (humaines, opérationnelles, ou de configuration). En outre, près de trois quarts des compromissions sont l'œuvre d'acteurs externes et 55 % relèvent du crime organisé.

Prises collectivement, les entreprises s'améliorent en matière de neutralisation des menaces, la majorité étant jugulées en quelques jours, voire moins. Pour autant, les cybercriminels semblent revoir leurs ambitions à la hausse : 72 % des compromissions frappent des grandes entreprises, même si plus de la moitié des victimes rapportent aussi une atteinte aux données personnelles. Si l'on en doutait encore, le cybercrime est avant tout un business à but lucratif : 86 % des attaques sont motivées par l'appât du gain et les ransomwares représentent 27 % des incidents par malware, toujours d'après notre rapport.

L'augmentation des compromissions s'explique en partie par la prolifération des terminaux, traditionnels et de machine à machine (M2M), notamment des capteurs et autres objets connectés (IoT). Avec près de 15 milliards d'appareils M2M connectés aux réseaux IP d'ici à 2023[3] , le ratio terminaux/utilisateurs devrait s'établir à un minimum de 3:1 sur cette même période. Évaluer l'impact des appareils IoT sur les réseaux actuels n'est pas chose aisée. Une chose est sûre, bon nombre de ces terminaux sortent d'usine avec des mots de passe élémentaires, et donc aisément piratables.

Réseaux 5G : fléau ou aubaine pour votre sécurité ?

Alors que les entreprises prévoient d'intensifier leur adoption de nouveaux services 5G, la réduction de leur exposition globale au risque devra passer par une réflexion sur leurs services, leurs terminaux et leurs processus de sécurité.

En substance, la 5G n'est qu'un moyen plus rapide et plus efficace de transférer du trafic IP via des connexions sans fil à faible latence. Elle ne présente donc pas en soi une nouvelle surface d'attaque. Toutefois, les réseaux privés 5G seront confrontés à des dangers de deux grands ordres, à savoir l'expansion progressive des menaces déjà présentes sur les réseaux 4G, et l'introduction de menaces totalement inédites tant dans leur conception que dans leur visée.

À l'heure où les réseaux 5G voient l'émergence de nouveaux cas d'usage, dont beaucoup étaient jusqu'alors l'apanage exclusif des réseaux filaires, les entreprises doivent redoubler de vigilance. Pensez à ces applications qui brassent d'énormes volumes de données et requièrent toujours plus d'interactions M2M via une myriade de terminaux sans fil. De telles applications créent un terreau favorable aux attaques à motivation financière et à l'espionnage industriel, sachant qu'un simple appareil IoT non géré représente une porte d'entrée au réseau.

Côté sécurité, la 5G capitalise sur les mesures en place pour la 4G, auxquelles viennent s'ajouter des innovations pour contrer les menaces inconnues et instaurer la confiance[4] . Parmi celles-ci :

- Chiffrement intégral des données utilisateurs intrabande et de la signalisation hors bande, rendant toute interception quasiment impossible sur les réseaux sans fil. Chaque accès est authentifié par le réseau domestique/fournisseur afin que le réseau de l'abonné en vérifie la légitimité.
- Vérification identique du réseau, qu'il s'agisse d'une connexion 5G ou Wi-Fi, pour éliminer les bornes non autorisées de type « IMSI-catcher » qui captent les identités internationales d'abonnement mobile des terminaux. Compatible avec tous les réseaux, cette méthode d'authentification améliore le contrôle du réseau domestique indépendamment du mode d'utilisation des terminaux. Elle bloque également les tentatives d'espionnage et de vol d'identifiants.
- Nouveau proxy SEPP (Secure Edge Protection Proxy) pour empêcher la propagation aux réseaux 5G des menaces présentes sur les réseaux connexes moins bien sécurisés.
- Découpage réseau (slicing) basé sur le SDN pour diviser logiquement le réseau physique en « tranches » virtuelles, chaque tranche comptant ses propres fonctionnalités réseau. Le trafic réseau présent sur une tranche peut alors être isolé des autres. Par le passé, la séparation du trafic et des fonctionnalités passait par la mise en place de réseaux physiques distincts. Grâce au slicing de la 5G, les prestataires peuvent plus précisément ajuster leurs fonctions réseaux et ainsi répondre aux besoins spécifiques de leurs applications. Ils peuvent notamment isoler les applications critiques au sein de tranches distinctes, les protégeant ainsi d'éventuelles attaques portées sur d'autres applications.

Le 3GPP (3rd Generation Partnership Project) est l'organisme chargé de la normalisation de la 5G. Ses missions couvrent notamment la protection des bornes, antennes et cœurs de réseau en appliquant les protocoles de sécurité d'organisations comme l'IETF (Internet Engineering Task Force) ou le NIST (National Institute of Standards and Technology). Le renforcement des standards 5G vise à éliminer les failles de sécurité des communications sans fil.

5G : bonnes pratiques de sécurité

En matière de protection des données, on ne peut jamais être trop prudent. Nous faisons ici le point sur les facteurs à prendre en compte pour bien planifier votre déploiement de la 5G.

Les frameworks de cybersécurité offrent une méthodologie pour appréhender les divers éléments d'un profil de sécurité et éviter ainsi toute improvisation. Ici, le Cybersecurity Framework du NIST fournit un excellent point de départ car il repose sur des standards largement adoptés et vise à réduire l'exposition aux cyber-risques des infrastructures d'importance vitale comme les réseaux 5G. Les entreprises sont ainsi mieux armées pour comprendre la somme prodigieuse d'éléments qui gravitent sur leur réseau et identifier les interfaces à risque. Parce qu'il dresse un plan de sécurité des données équilibré qui intègre l'ensemble des vecteurs d'attaque (composants, interfaces, points de transition, etc.), un tel framework peut constituer votre première ligne de défense.

Le chiffrement doit être omniprésent. En ce sens, la 5G permet un chiffrement de bout en bout, tant pour la signalisation des configurations que pour le transfert de données utilisateurs. Toutefois, cette fonctionnalité doit être activée pour être effective. Veillez d'abord à ce que les données et la signalisation soient chiffrées par défaut, puis adoptez une approche « zero trust » pour chaque application. Concrètement, la moindre transaction doit être authentifiée pour garantir une sécurité maximale sur l'ensemble des données et communications vocales, quel que soit leur niveau de confidentialité. Dans cette optique, les notions de périmètre et de cercle de confiance sont à proscrire, et la fiabilité d'un individu ne peut jamais être tenue pour acquise. Les réseaux actuels sont en effet si complexes qu'il est tout bonnement impossible de savoir où placer la limite.

Tout aussi essentiel que le respect des standards : bien comprendre la supply chain qui entoure la 5G. Les entreprises doivent s'approvisionner auprès de fournisseurs reconnus pour tous leurs équipements 5G – jusqu'au niveau des puces – en s'assurant de l'absence complète de backdoors sur ces appareils. De même, chaque organisation veillera à bien saisir les enjeux de sécurité que présentent les firmwares et autres logiciels sur ces équipements 5G. Pas question, par exemple, que ces programmes permettent à un malware open-source présent sur un référentiel de code d'infecter des appareils, voire le cœur de réseau 5G d'un opérateur.

Enfin, chaque entreprise doit adopter des bonnes pratiques pour protéger l'ensemble de ses applications. Voici quelques principes préconisés par les leaders du secteur :

Séparation des responsabilités – Cette mesure empêche un individu de subvertir à lui seul tout un système de sécurité.

Contrôle des accès basé sur les rôles – La connexion aux informations et aux ressources est limitée aux seuls rôles utilisateurs et applications nécessitant un accès.

Principe du moindre privilège – S'agissant des privilèges d'accès, les utilisateurs doivent ne bénéficier que des droits strictement nécessaires à la réalisation de leurs tâches.

Authentification multifacteur – Pour améliorer votre sécurité globale, privilégiez autant que possible l'authentification à deux facteurs ou plus pour les connexions à distance.

Modernisation – N'oubliez pas de mettre à jour les éventuelles ressources plus anciennes et non gérées rattachées à votre réseau. Veillez aussi à la bonne protection des appareils ou capteurs d'ancienne génération, dans la mesure où ils fragilisent la sécurité de votre réseau.

Gouvernance – Avec l'augmentation des wearables à usage médical, le respect des réglementations sur la gouvernance des données (loi HIPAA aux États-Unis, normes PCI...) constitue l'un des autres grands enjeux de la 5G. En se rapprochant de leurs fournisseurs d'équipements, logiciels et réseaux, les entreprises veilleront à ce que ces objets connectés ne deviennent pas le maillon faible de leur chaîne de sécurité des données.

La solution Verizon

Verizon s'impose comme l'une des forces motrices de la 5G, comme en témoigne le nombre important d'entreprises qui nous ont choisis pour cette étape importante de leur développement. Hormis son réseau de 2 000 magasins rien qu'aux États-Unis, Verizon possède un maillage international particulièrement dense. Notre entreprise est elle-même l'un des primo-adoptants de la 5G, ce qui nous a permis d'affermir nos pratiques de sécurité au regard des réglementations PCI, HIPAA et bien d'autres encore. Naturellement, cette expérience vient nourrir notre offre de produits et services à travers le monde.

Chez Verizon, la sécurité fait partie intégrante de notre écosystème 5G. Nos mécanismes de protection obéissent à un processus strict de sélection des fournisseurs et des produits. Nous regardons au-delà des seules fonctionnalités pour concevoir un modèle de produits avec contrôles de sécurité intégrés. Une telle approche passe par le renforcement de la sécurité des appareils, mais aussi des supply chains physiques et digitales. Ainsi, lorsque nous publions les mises à jour et correctifs logiciels de fournisseurs, nous veillons toujours à leur parfaite intégrité et à l'absence de faille.

Nous sommes fiers de collaborer avec de grands noms du secteur et organismes de sécurité. Membre fondateur de deux organisations pionnières de la sécurité 5G – le CSDE (Council to Secure the Digital Economy) et l'alliance O-RAN – Verizon s'engage à mener de front les initiatives mondiales pour la sécurité de l'IoT et le déploiement d'antennes et de bornes 5G virtuelles, ouvertes, interopérables et standardisées. Nous travaillons également en partenariat avec le Communications ISAC (Information Sharing and Analysis Center)4 . Placé sous l'égide du ministère américain de la sécurité intérieure, cette entité offre un espace de dialogue à une pluralité d'acteurs (organismes de sécurité, entreprises de communication, partenaires gouvernementaux américains…) pour le déploiement d'infrastructures et services de communication fiables et sécurisés à travers le pays.

Dans cette optique, Verizon s'appuie sur les standards 3GPP régissant les architectures de sécurité de la 5G. Ces standards incluent des recommandations de l'IETF et du NIST, comme par exemple l'authentification mutuelle entre terminaux utilisateurs et bornes 5G pour bloquer les accès frauduleux et l'interception d'identifiants (puisque rien, ni la signalisation, ni les données, ne doit être transmis en clair sur les réseaux sans fil).

Ce n'est pas tout. Nous nous assurons que nos smartphones et autres équipements 5G répondent à la fois aux normes sectorielles et à nos propres exigences et processus de sécurité des appareils. Ainsi, nous imposons l'utilisation d'une carte SIM UMTS (système universel de télécommunications mobiles)4 dotée d'un système de scellé pour prévenir l'exposition des identifiants stockés sur la puce (authentification du réseau, identifiants de connexion de l'abonné…).

Ensuite, grâce à une série de tests automatisés, nous analysons, inspectons et utilisons des configurations standardisées pour bâtir un réseau 5G sécurisé autour de chaque composant, y compris les téléphones, routeurs et appareils MiFi. Chacun de ces composants doit par ailleurs être doublement conforme aux standards en vigueur et à nos propres exigences draconiennes de sécurité des terminaux.

Nos services 5G reposent sur une nouvelle architecture SDN capable d'isoler différents services et applications au sein de tranches distinctes de ressources et de trafic. Notre dispositif renforce la sécurité des entreprises à la manière des VPN, à la différence près qu'il simplifie les processus d'allocation et d'isolement. Les entreprises ont ainsi la possibilité de séparer et protéger leurs systèmes critiques des appareils IoT non gérés, de sorte que leurs systèmes vitaux restent à l'abri des attaques DDoS.

Avec à son actif plusieurs décennies d'expérience dans le déploiement et la gestion de réseaux d'entreprise, Verizon applique aujourd'hui toute cette expertise et ces savoir-faire aux appareils et réseaux 5G. Nous mettons en œuvre les outils, les produits et les équipes indispensables pour aider nos partenaires et nos utilisateurs à ajuster leurs stratégies de sécurité au fil de l'évolution de la 5G.

Prochaines étapes
Première entreprise à commercialiser un service mobile 5G, Verizon vous accompagne dans la sécurisation de votre environnement 5G. Pour découvrir comment la 5G Verizon vous aide à consolider le profil de sécurité de votre entreprise, contactez votre conseiller Verizon.

verizon

1 « The Future of IoT Miniguide: The Burgeoning IoT Market Continues », Cisco, 19 juillet 2019.

2 « Rapport 2020 sur les compromissions de données », Verizon, 2020.

3 « Cisco Annual Internet Report (2018–2023) », Cisco, 9 mars 2020.

4 « First Principles for Securing 5G », Verizon, décembre 2019.