



Prédictions IoT pour

# 2024 et au-delà.

L'essor de la périphérie intelligente.

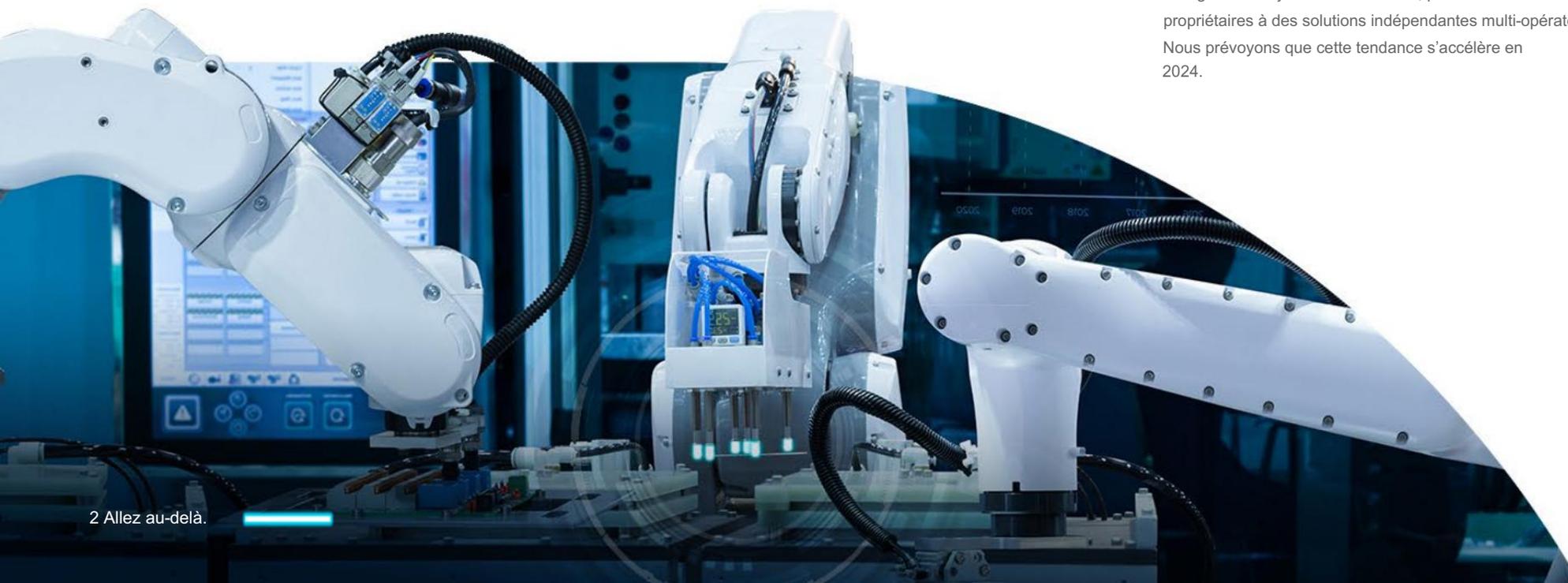


# Prédictions IoT pour 2023 : comment avons-nous fait ?

Par Nick Earle, PDG et Larry Socher, vice-président directeur de la stratégie et des alliances chez Eseye.

Notre rapport IoT Predictions for 2023 and Beyond, publié fin 2022, était peut-être le plus audacieux à ce jour. Nous avons prédit que le secteur était à l'aube d'un point d'inflexion majeur et que 2023 serait « l'année où le contrôle passera de l'opérateur de réseau à l'entreprise et à l'appareil ».

Avant de faire nos prévisions pour 2024, voyons comment nous nous en sommes sortis avec chacune de ces tendances :



## un

[Fissures du verrouillage propriétaire MNO :](#)

Comme prévu, 2023 a vu une demande accrue de la part des ORM pour adopter de nouvelles plates-formes cloud natives eSIM mondiales. Cela s'est produit pour deux raisons. Le premier était l'adoption croissante des eSIM compatibles eUICC par les clients finaux, ce qui a considérablement réduit la demande de cartes SIM MNO propriétaires verrouillées sur leur réseau.

Le second était le transfert de l'IoT d'Ericsson

Plate-forme d'accélérateur (anciennement DCP) à Aeris, ce qui a marqué la fin de l'investissement et du support d'Ericsson pour les anciennes solutions de gestion de la connectivité des MNO. Ceci, combiné à l'annonce précédente par Vodafone de la scission de son activité GDPP et au prochain

sortie de la [norme SGP.32](#), a marqué le début d'un changement majeur dans l'industrie, passant de solutions propriétaires à des solutions indépendantes multi-opérateurs. Nous prévoyons que cette tendance s'accélère en 2024.

## deux

[Interopérabilité entre les publics et réseaux privés :](#)

L'accent est de plus en plus mis sur l'itinérance entre réseaux publics et privés pour des cas d'utilisation tels que entreposage et exploitation minière. Cependant, l'adoption a été plus lent que prévu en raison de l'intégration défis, difficultés d'opérationnalisation et un manque de normes.

«...changement majeur dans l'industrie solutions propriétaires du fournisseur aux agnostiques interopérabilité multi-opérateurs.

## trois

[Ascendance du multi-RAT :](#)

Les clients utilisent de plus en plus [plusieurs technologies d'accès radio \(RAT\)](#) pour résoudre les problèmes. Par exemple, Telli Health propose des solutions cellulaires et LoRaWAN pour les applications à distance.

surveillance des patients et, ce faisant, est rapidement devenue la principale solution de gestion à distance des patients aux États-Unis. Nous prévoyons qu'à l'avenir, ceux-ci convergeront vers une seule solution et que les cas d'utilisation de dispositifs multi-RAT s'accéléreront.

à mesure que l'intelligence se déplace vers l'Edge, nous nous attendons à ce que la recharge des véhicules électriques à domicile ouvre la voie avec des déploiements bimodèles de WiFi domestique et d'unités cellulaires.

« Nous nous attendons à ce que les cas d'utilisation d'appareils multi-RAT s'accélèrent à mesure que l'intelligence se déplace vers la périphérie... »

## quatre

Convergence consommateur/entreprise :

La convergence des consommateurs et des entreprises dans la maison numérique gagne du terrain, mais elle en est encore au début du cycle d'adoption.

« ... la convergence des consommateurs et des entreprises dans la maison numérique gagne du terrain... »

Les exemples incluent l'intégration de déploiements grand public et d'entreprise dans les systèmes de sécurité domestique, comme le partenariat d'ADT avec Google Nest pour les solutions DIY.



## cinq

L'IoT commence et se termine avec l'appareil :

Conscients de l'importance de la connectivité des appareils IoT, nous avons lancé notre SMARTconnect™ les logiciels et l'IoT

Programme de services LaunchPad pour garantir des déploiements réussis. L'accent mis sur une conception appropriée des appareils a entraîné une croissance substantielle des solutions Device Intelligence, avec des retours positifs de la part des clients et des partenaires. Cette prédiction s'est avérée exacte dans notre enquête portant sur plus de 1 000 projets de déploiement IoT dans le monde, qui a révélé que le défi numéro un de l'IoT pour plus de 80 % des personnes interrogées était la conception et l'optimisation du micrologiciel des appareils, et non la connectivité de base.

Ces tendances fournissent des informations permettant de prédire les évolutions futures en 2024.

Même si nous n'avons certainement pas tout fait correctement, nous sommes très fiers des prévisions de l'année dernière et pensons que 2023 sera "l'année où le contrôle est passé du réseau l'opérateur à l'entreprise et à l'appareil.

Alors, qu'est-ce que cela signifie pour 2024 et au-delà ?



# Prédictions IoT pour 2024 et au-delà : l'essor de l'intelligence IoT à la périphérie.

Sachant que les prévisions de l'année dernière étaient extrêmement perturbatrices et que le secteur était confronté à un transfert massif de pouvoir de l'opérateur de réseau mobile vers l'entreprise, nous avons décidé cette année d'adopter une approche différente et de nous concentrer davantage sur l'une de nos principales observations du secteur : l'accent est mis sur l'appareil. C'est pour cette raison que nous appelons 2024 « l'année de l'Edge IoT Intelligent » et prévoyons une attention accrue portée à la « résilience » et à la « confiance ».

Il s'agit d'une évolution signalée depuis de nombreuses années.

En 2016, Santhosh Rao de Gartner prédisait que « d'ici 2025, 75 % des données générées par les entreprises seront créées et traitées en dehors d'un centre de données ou d'un cloud traditionnel. »<sup>1</sup> Si

Dans une direction correcte, cela signifie que les appareils IoT et les passerelles Edge seront de plus en plus intelligents et assumeront un pourcentage de traitement en augmentation exponentielle.



**75%**  
traitement des données  
générées par l'entreprise

Mais pour que ce transfert de traitement du centre de données traditionnel vers l'Edge se réalise, il faudra une connectivité beaucoup plus flexible, résiliente et intelligente (ou « plus intelligente ») entre l'appareil, l'Edge et le cloud.

Chacune de nos prévisions pour 2024 et au-delà se concentre d'abord sur l'augmentation de l'intelligence et du traitement à la périphérie, puis met en évidence la nécessité d'une connectivité plus intelligente pour permettre ce changement de traitement. Ils amplifient le besoin croissant d'adopter le concept « [Connecté par le design](#) » principes et [l'importance](#) d'augmenter l'intelligence des appareils et de Edge.

« ... il faudra une connectivité beaucoup plus flexible, résiliente et intelligente (ou « plus intelligente »)... »

À mesure que les données en périphérie deviennent de plus en plus critiques pour l'entreprise, la mission et la vie pour prendre en charge des cas d'utilisation tels que les soins de santé à distance, les paiements financiers, la gestion distribuée de l'énergie et le commerce du carbone, nous devons également étendre la confiance à l'Edge.

Comme nos trois prévisions pour 2024 sont centrées sur les appareils, nous avons adopté une approche différente pour le rapport de prévisions de cette année.

Nous avons approfondi chacun d'entre eux de manière beaucoup plus approfondie pour illustrer pourquoi tous les chemins mènent au dispositif intelligent.

Cela ne devrait pas surprendre. C'est la conséquence naturelle du déplacement de l'intelligence vers l'Edge, et finalement vers l'appareil IoT lui-même. Cela perturbera énormément le paysage de l'Edge IoT, car les opérateurs se démènent pour développer des capacités centrées sur les appareils et les MVNO sont obligés de décider s'ils doublent leur valeur en offrant aux clients des solutions et des services d'appareils avancés, ou s'ils continuent à se concentrer sur les cartes SIM de base basées sur le volume. et des données vendues sur un site Web. Dans ce nouveau monde, nous positionnons clairement Eseye comme un acteur de valeur et pensons que « tout commence et se termine avec l'appareil ».

# Prédiction 1

## Un nouveau logiciel de connectivité intelligente reliera la périphérie et le cloud.



Nous prévoyons que 2024 sera l'année où nous verrons l'émergence de logiciels de communication qui fourniront une « connectivité intelligente » reliant l'intelligence Edge et le cloud.

Le traitement et la prise de décision des appareils et des périphéries continuent de s'accélérer malgré le ralentissement de la loi de Moore. Les cas d'utilisation de l'IoT continuent de regrouper et de traiter ces données dans le cloud pour générer une analyse et une valeur supplémentaires. Bien qu'un pourcentage plus important du traitement et de l'analyse ait lieu à la périphérie, ce sont généralement l'aide à la décision et les actions back-end dans le cloud qui déterminent la plupart des décisions critiques pour l'entreprise, la mission ou la vie.

Un bon exemple est d'avoir un capteur d'eau intelligent, compatible avec l'apprentissage automatique (ML), qui peut être adapté à l'humidité d'une pièce. Bien que le capteur puisse avoir assez de logique pour déterminer le seuil qui est au-dessus de la normale, alerter quelqu'un d'une fuite afin que ils peuvent agir avant qu'une maison ne subisse des dégâts d'eau importants les dégâts sont généralement causés à partir du cloud.

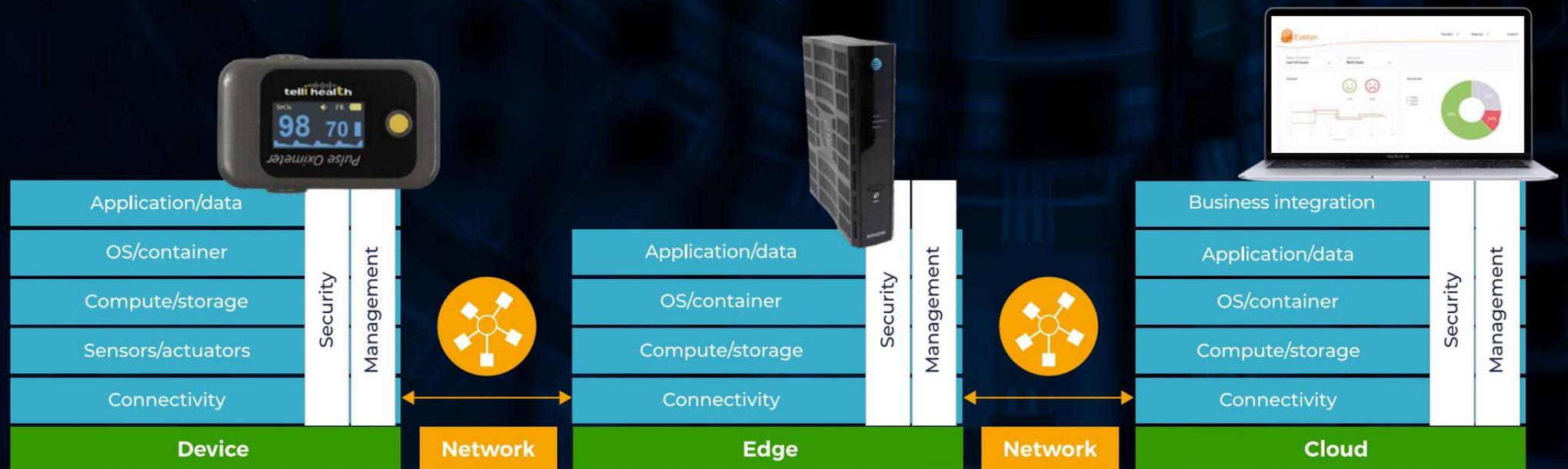
« Le traitement et la prise de décision des appareils et des périphériques continuent de s'accélérer... »

Pour prendre en charge cette intelligence distribuée, il est nécessaire de combiner l'intégration full-stack dans le Appareils IoT, collectant et traitant des informations sur l'appareil, ainsi qu'une connectivité appareil-cloud sécurisée et résiliente, reliant les appareils vers et via Edge dans le cloud.

Comme illustré dans le modèle ci-dessous, pour fournir une solution de surveillance à distance des patients sécurisée, conforme (c'est-à-dire HIPAA) et fiable, nous devons d'abord fournir une intégration complète depuis les capteurs d'un moniteur cardiaque, en passant par le calcul et le stockage, le système d'exploitation et les conteneurs. tout au long des données, des applications et du ML qui s'exécutent sur l'appareil, avec toute la sécurité et la gestion nécessaires pour garantir que l'appareil n'est pas falsifié et que les données ne sont pas compromises.

Nous devons ensuite nous assurer que nous disposons d'une connectivité sécurisée et résiliente depuis l'appareil, via le réseau et vers le cloud, où les données peuvent être traitées, analysées et surveillées, déclenchant des alertes aux professionnels de la santé pour qu'ils prennent des mesures pour prévenir ou réagir rapidement. une crise cardiaque.

« ...une connectivité sécurisée et résiliente depuis l'appareil... vers le cloud... »



## Prédiction 1 suite.

Pour relier l'intelligence de l'appareil IoT aux analyses de surveillance de l'état et aux tableaux de bord opérationnels dans le cloud, vous avez besoin d'une connectivité intelligente ou « intelligente » intégrée à l'appareil qui permet une connexion sécurisée, conforme et résiliente de l'appareil au cloud.

La connectivité intelligente sur l'appareil doit gérer la configuration et les performances de la connectivité, en sélectionnant la meilleure technologie réseau et le meilleur fournisseur (par exemple, WiFi domestique/ haut débit, cellulaire, satellite R17 NTN) en fonction de multiples contraintes telles que la disponibilité, la bande passante, la latence, la force du signal, le coût, la puissance et la sécurité.

**"La connectivité intelligente sur l'appareil doit gérer la configuration et les performances de la connectivité..."**

Idéalement, cette bibliothèque de connectivité devrait fournir une instrumentation améliorée des appareils et des réseaux, et la visibilité pour maximiser l'état de l'appareil et pour aider à sectionner et résoudre les problèmes, y compris les protocoles de communication de bout en bout pour les appareils.

visibilité et performances vers le cloud. Il doit fournir des liens de corrélation avec les données du réseau, du cloud, des applications et de la santé, pour permettre une gestion complète des services de l'appareil au cloud. Il doit également fournir des instruments et des alertes pour permettre aux appareils et systèmes de gestion de la sécurité des données (SIEM).

**« Idéalement, cette bibliothèque de connectivité devrait fournir une instrumentation améliorée des appareils et des réseaux avec une visibilité et des performances de l'appareil au cloud. »**

Enfin, il doit intégrer l'authentification, l'autorisation, le cryptage, la gestion des clés et des données, le routage sécurisé et l'auditabilité pour permettre la sécurité (c'est-à-dire l'authenticité, l'intégrité, la confidentialité, la disponibilité) et la conformité (c'est-à-dire RGPD, PCI, HIPAA, ISO-14064). -2). Et il doit être géré depuis le cloud, mais avec suffisamment d'intelligence embarquée pour pouvoir récupérer la connectivité en cas de panne de réseau.

**En résumé, 2024 marquera le début de bibliothèques de logiciels de communication « Smart Connectivity » reliant l'intelligence Edge et l'intelligence cloud.**

## Prediction 2

# La connectivité intelligente alimente le traitement distribué des données pour l'IoT et jette les bases de la 5G.



Nous prévoyons que 2024 sera l'année où nous verrons l'émergence de solutions logicielles de communication sur les appareils qui fourniront la « connectivité intelligente » qui alimente le traitement distribué des données pour l'IoT et jette les bases de la 5G.

À mesure que la puissance de calcul augmente à la périphérie, l'une des grandes questions que les concepteurs de systèmes doivent résoudre est de savoir où traiter les données. Dans certains cas où la latence est critique, par exemple lorsque vous devez analyser un flux vidéo et émettre immédiatement un avertissement si quelqu'un est en danger, le ML de vision par ordinateur devra clairement s'exécuter en périphérie.

Mais qu'en est-il des applications qui ne sont pas aussi sensibles au facteur temps ? Par exemple, que se passe-t-il si vous disposez d'une application d'assurance automobile qui reçoit des données de caméras vidéo et d'ordinateurs de bord et traite les données pour voir si le conducteur accélérât ou freinait excessivement juste avant un accident ? Et si la même solution était utilisée pour

la maintenance prédictive d'un véhicule pour déterminer quand il doit être entretenu et intervenir en cas d'urgence en cas d'accident ?

Pour chacune de ces demandes, où vous traitez les données, sur l'appareil ou dans le cloud, peuvent être un fonction du type et du coût de la connectivité à ce moment-là.

Considérons un cas d'utilisation dans lequel nous regroupons des données à partir des flux vidéo et de l'instrumentation de la voiture à l'aide d'un appareil de communication doté de deux radios : une radio WiFi pour utiliser le réseau domestique du conducteur et connexion haut débit depuis le garage et un modem cellulaire compatible satellite pour les réseaux mobiles terrestres publics sur les routes en itinérance par satellite pour les endroits éloignés au-delà de la couverture terrestre.

Le réseau WiFi a le plus de bande passante et pas de frais supplémentaires. Le réseau mobile terrestre a un peu moins de bande passante et entraîne des dépenses. La connexion par satellite a une bande passante nettement inférieure et est coûteuse. Pour cette raison, nous pouvons traiter davantage de données localement et transmettre différentes quantités de données en fonction des disponibilités. connectivité.

**"Pour chacune de ces applications, où vous traitez des données, sur l'appareil ou dans le cloud, cela peut dépendre du type et du coût de la connectivité du moment."**

Par exemple, si nous conduisons dans une zone avec une mauvaise couverture cellulaire et ne disposons que d'une connectivité par satellite, nous utiliserons le calcul local pour analyser les données et transmettrons uniquement les informations critiques sur la faible bande passante. connexion par satellite. Lorsque vous utilisez le réseau cellulaire, nous pouvons envoyer des mises à jour plus fréquentes sur les performances du moteur et la sécurité du conducteur, y compris des photos occasionnelles ou de courtes vidéos. De retour au garage avec WiFi, nous pouvons transmettre plus de données et télécharger des vidéos pour une analyse détaillée dans le cloud.



## Prédiction 2 suite.

Pour résoudre les défis liés à la connexion aux réseaux de plusieurs opérateurs en fonction de la disponibilité, de la force du signal et de la latence, nous avons besoin d'un logiciel de connectivité intelligent qui bascule de manière transparente entre les technologies et les réseaux. Le logiciel doit également tenir compte du coût et éviter d'envoyer des données excessives via des connexions coûteuses. Les API du logiciel peuvent être utilisées par des applications et des solutions de gestion de données distribuées pour déterminer où traiter les données, quelles données pour transmettre et prioriser les données critiques.

De plus, le logiciel devrait permettre une gestion plus intelligente de l'appareil, « sensible au réseau », en conservant les mises à jour et les correctifs de sécurité lorsque la voiture est sur le réseau domestique afin d'éviter des mises à jour coûteuses.

Enfin, au cours des dernières années, nous avons beaucoup entendu parler de la puissance de l'URLCC 5G et de la façon dont la QoS et le découpage du réseau peuvent être exploités pour permettre des cas d'utilisation extrêmement difficiles tels que la réalité augmentée (RA) pour la télémédecine et la chirurgie à distance. Cependant, il y a eu très peu de discussions sur la façon dont vous pourriez mettre en œuvre ces fonctionnalités dans un modèle fédéré multi-opérateurs.

**"...La qualité de service et le découpage du réseau peuvent être exploités pour permettre des cas d'utilisation extrêmement difficiles tels que la réalité augmentée (RA)..."**

C'est beaucoup plus difficile qu'une solution à opérateur unique et, à notre avis, cela ne sera possible qu'en activant les composants centraux de l'intelligence au niveau du seul composant architectural commun : le dispositif. La même intelligence sur l'appareil permet un traitement de données distribué qui est nécessaire pour signaler à chaque réseau mobile d'établir les ressources appareil vers le cloud pour maintenir une session et assurer une surveillance continue de l'état et des performances du réseau afin de garantir une haute résilience et une faible latence.

connectivité vitale.

**"La même intelligence sur l'appareil qui permet le traitement distribué des données est nécessaire pour signaler à chaque réseau mobile d'établir l'appareil vers le cloud."**

Toutes ces exigences seront beaucoup plus faciles à mettre en œuvre une fois dans l'appareil que plusieurs fois auprès d'opérateurs de réseaux disparates, avec tous les coûts et la complexité associés.

C'est pour cette raison pratique que nous prévoyons que « 2024 sera l'année où la « connectivité intelligente » centrée sur les appareils jouera un rôle clé en permettant le traitement distribué des données pour l'IoT et en jetant les bases de la 5G.



## Prédiction 3

# La connectivité intelligente comme base de la sécurité, de la conformité et de la confiance entre appareils et cloud.



Nous pensons que les technologies sous-jacentes sont disponibles et prévoyons que 2024 sera l'année où nous verrons l'émergence de bibliothèques de logiciels fournissant la connectivité intelligente pour garantir la sécurité et la conformité de l'appareil au cloud et préserver la confiance.

Alors que l'IoT devient de plus en plus critique pour l'entreprise, la mission et la vie avec des cas d'utilisation émergents, notamment la vente et les paiements, le suivi des actifs et de la flotte, la surveillance à distance des patients et la sécurité incendie, il devient de plus en plus nécessaire de protéger et de comptabiliser les données.

En conséquence, de plus en plus d'appareils et de cas d'utilisation doivent désormais non seulement sécuriser leurs données contre les acteurs malveillants pour s'assurer qu'ils ne volent pas ou ne modifient pas les données, mais doivent également acheminer en toute sécurité les données qui restent souvent dans un pays ou une région (UE). respecter la souveraineté des données et toute autre conformité en vigueur. Cela nécessite une combinaison de sécurité sur l'appareil et sur le réseau, y compris l'authentification, l'autorisation, la clé de chiffrement et les données.

gestion, ainsi qu'un routage sécurisé des appareils vers le cloud et une audibilité pour répondre aux directives de conformité. Cela nécessite également un cadre robuste pour gérer l'appareil et fournir une instrumentation et une audibilité aux systèmes de sécurité et de conformité des couches supérieures.

### "...nécessite une combinaison de sécurité sur l'appareil et sur le réseau..."

Un bon exemple de ces cas d'utilisation est le marché carbone. Compte tenu du taux élevé de fraude sur les marchés des crédits carbone, un chargeur de véhicule électrique ou tout autre appareil souhaitant participer aux bourses du carbone devra

garantir que les données générées à partir d'un appareil sont entièrement vérifiables, exactes et n'ont pas été falsifiées lors du transit de l'appareil vers l'échange. Cela nécessite une combinaison de sécurité complète sur l'appareil, de chiffrement complet de l'appareil vers le cloud avec un routage sécurisé et de blockchain ou de technologies similaires pour garantir l'intégrité et l'audibilité afin de répondre aux exigences strictes de l'ISO et d'autres cadres réglementaires.



# Prédiction 3 suite.

De même, tout appareil ou cas d'utilisation transmettant des données personnelles devrait être protégé par le RGPD. Les données de santé seraient soumises à une conformité similaire, notamment HIPAA et PCI sur les transactions financières.

Pour prendre en charge le commerce du carbone et d'autres cas d'utilisation sensibles, vous aurez besoin d'un logiciel de connectivité intelligent, résident sur l'appareil, qui :



**Permet** l'authentification, l'autorisation, le cryptage, la gestion des clés et des données sur l'appareil.



**Protège** les clés de l'appareil, du réseau et des applications dans l'enclave sécurisée d'un module de plateforme sécurisée (TPM) ou d'une carte SIM alignée sur IoT SAFE ou des normes similaires.



**Agit** comme un agent implicite sur l'appareil, fournissant une instrumentation pouvant être utilisée pour les systèmes de gestion de la sécurité des appareils et des données (SIEM) (par exemple, utilisation du processeur supérieure à 90 % pendant 5 minutes, nouvelle source/destination IP, nouvelle recherche DNS).



**S'intègre** aux technologies et opérateurs de réseau sous-jacents et fonctionne avec les réseaux définis par logiciel (SDN) pour fournir un routage et une auditabilité sécurisés dans la région afin de permettre la sécurité et la conformité en tirant parti de la blockchain ou de technologies similaires.

« ... la transmission de données personnelles devrait être protégée... »

"...fonctionne avec le logiciel Réseaux définis (SDN) pour fournir un routage et une auditabilité sécurisés dans la région..."

Pour ces raisons, et sur la base de nos deux premières prédictions, nous pensons que « 2024 sera l'année où la « connectivité intelligente » jettera les bases de la sécurité, de la conformité et de la confiance entre les appareils et le cloud.



## Conclusion:

# 2024 sera l'année des logiciels de connectivité intelligente.



Les entreprises numériques évoluent rapidement et répartissent la manière dont elles traitent les données. Cette trajectoire signale un changement convaincant, prophétisé par les analystes, selon lequel 75 % de toutes les données seront traitées en périphérie d'ici 2025. Nos prévisions pour 2024 soulignent clairement la nécessité de solutions logicielles de connectivité intelligentes pour fournir une base au traitement Edge, garantir la confiance, et garantir la résilience des applications métier, de mission et vitales pour faire de cet objectif une réalité.

Cela nécessitera un logiciel de connectivité portable, léger et suffisamment flexible pour fonctionner sur une grande variété d'appareils, de systèmes d'exploitation et de modems. Il devra fournir un accès transparent et une commutation entre le plus grand nombre de réseaux cellulaires mondiaux et régionaux, ainsi que d'autres technologies, notamment le satellite, le WiFi, le Bluetooth, Zigbee et LoRa. Le logiciel doit être configuré et géré par une puissante plate-forme de gestion de la connectivité qui utilise le ML pour optimiser la connectivité en fonction de la disponibilité, de la résilience, de la bande passante, de la latence, de la puissance, de la sécurité et du coût afin de garantir qu'elle est adaptée aux besoins.

exigences uniques de chaque appareil et application.

En 2024 et au-delà, le besoin d'une solution de connectivité intelligente pour prendre en charge cette croissance exponentielle du traitement des données en périphérie n'a jamais été aussi important.

**Pour nous parler des tendances et des prévisions soulevées dans ce rapport ou discuter d'un prochain projet de connectivité IoT sur lequel vous travaillez, veuillez nous contacter.**



Prédictions IoT pour 2024 et au-delà.

## À propos de Eseye

En tant que leader mondial des solutions de connectivité IoT, nous appliquons notre expertise approfondie en matière d'appareils IoT pour aider les entreprises à tirer une valeur durable de leurs projets mondiaux. Nous travaillons en étroite collaboration avec nos clients, de l'idée à la mise en œuvre et au-delà, pour fournir une connectivité proche de 100 % à des millions d'appareils à travers le monde.

Nous voyons l'IoT différemment. Nous commençons toujours par l'appareil. En adoptant cette approche, nous avons réalisé des projets réussis dans tous les secteurs pour des marques mondiales telles que Shell, Amazon et Bosch.



amazon

BOSCH

Nos solutions de connectivité IoT primées à plusieurs reprises, y compris l'eSIM AnyNet+ IoT et iSIM, le matériel Hera IoT, le logiciel de connectivité intelligente AnyNet SMARTconnect™ et la plateforme cloud native Infinity IoT Connectivity Management Platform™, nous permettent de concevoir et de mettre en œuvre avec succès des projets IoT mondiaux de toute ampleur ou complexité. Nous sommes soutenus par un puissant écosystème de partenaires, connectant de manière transparente des appareils dans 190 pays, restant indépendants du réseau en

exploitant plus de 700 réseaux mondiaux disponibles. Nous sommes connus pour nos premières sur le marché, notamment Zigbee, la carte SIM multi-IMSI et maintenant le premier IoT Readiness Level (IRL) Framework™ du secteur, qui accélère le déploiement de projets IoT grâce à notre programme de service flexible IoT LaunchPad.

Notre gamme avancée de solutions et de services de connectivité IoT a été renforcée renforcé par notre reconnaissance en tant que visionnaire dans le Magic Quadrant™ Gartner® 2023 pour les services de connectivité IoT gérés, dans le monde entier. Personne ne le fait mieux l'IoT de bout en bout.

En savoir plus : [www.eseye.com](http://www.eseye.com)

"Il devra fournir un accès transparent et une commutation entre le plus grand nombre de réseaux cellulaires mondiaux et régionaux..."



eseye

# Aller au-delà.

Pour parler à Eseye des prédictions soulevées dans ce rapport ou discuter d'un projet IoT actif ou à venir, veuillez...

Contactez-nous

 [Youtube](#)

 [LinkedIn](#)

 [www.eseye.com](http://www.eseye.com)