

Mots clés : APN, IoT, M2M, Sécurité

Communiqué de presse

Comment connecter ses objets en toute sécurité ?

Montpellier, le 28 Novembre 2019,

Selon le cabinet d'analyses Juniper Research, le nombre d'objets connectés est déjà plus de deux fois supérieur à la population mondiale¹. **La sécurité, la collecte et l'analyse de données en temps réel** deviennent ainsi des **enjeux fondamentaux** dans un contexte de montée en puissance de l'**IIoT (Internet Industriel des objets)**. En effet, il est à noter que les attaques sur des dispositifs IoT auraient été multipliées par 9 entre le premier semestre 2018 et le premier semestre 2019 en passant de 12 millions à 105 millions²... Afin de pallier ces offensives, la société Matooma a créé une solution – le **MatooWan** – permettant de déployer ses objets connectés en alliant sécurité, maintenance et supervision à distance.

Industrialisation et sécurité : quels liens ?

L'**industrie 4.0** fait référence à la quatrième révolution industrielle et désigne « *une nouvelle génération d'usines connectées, robotisées et intelligentes* »³. Ce concept exprime l'idée d'une interconnexion, d'une **interaction entre les collaborateurs, les machines et les produits** à la suite de l'introduction de nouvelles technologies au sein des usines. Dans ce contexte, la sécurité fonctionnelle et la sécurité de l'information deviennent des enjeux primordiaux et jouent un rôle clé dans le développement des usines 4.0⁴.

Lors d'un projet d'industrialisation, plus le nombre d'équipements augmente, plus les failles potentielles de sécurité grandissent. Il est donc très important de limiter au maximum les risques, et surtout de bien **sécuriser l'échange de données entre l'objet communicant, les infrastructures télécom et le système d'information**. La mise en place d'un APN (Acces Point Name) privé permet d'assurer ce lien sécurisé à l'aide de cartes SIM M2M.

Sécuriser la connexion entre l'objet et le système d'information

Au cours du déploiement d'un projet IoT, il est possible de **connecter un objet par Internet ou via un réseau privé**. Dans ce dernier cas, afin de mêler maintenance à distance et sécurité, deux alternatives sont envisageables : l'**APN privé mutualisé** et l'**APN privé dédié**. Les deux solutions permettent d'accéder à un réseau sécurisé non visible sur Internet mais la seconde donne la possibilité de personnaliser totalement l'APN.

Cette technologie permet **une sécurisation, une maintenance et une supervision à distance en temps réel de la connectivité des objets industriels**. De ce fait, des entreprises font appel aux services d'un réseau

¹ <https://www.juniperresearch.com/press/press-releases/iiot-connected-devices-to-triple-to-38-bn-by-2020>

² <https://securelist.com/iiot-a-malware-story/94451/>

³ <https://www.visiativ-industry.fr/industrie-4-0/>

⁴ Korfmacher Sebastian, Mattiuzzo Corrado, « Passage à l'industrie 4.0 : les aspects liés à la sécurité ». Revue Hygiène et Sécurité du travail, 2017, NO 18.

privé pour le déploiement de leurs objets connectés afin de sécuriser les connexions et faciliter l'accès à distance des équipements. La société **Matooma** a répondu à la demande du marché IoT et a conçu sa solution d'APN privé : le **MatooWan**

La solution MatooWan, le réseau privé sécurisé de Matooma certifié par 2Gi Technologie

Le MatooWan est un **réseau privé sécurisé** qui répond aux différentes problématiques liées à l'industrialisation d'un projet IoT. Cette solution permet de **sécuriser le transfert des données** de l'objet connecté jusqu'au système d'information du client. Les **flux de données sont privés** (non visibles sur Internet) **et maîtrisables** : le volume de données ne pourra être augmenté par des attaques extérieures, limitant ainsi toute surconsommation de ses équipements.

Le MatooWan confère également la possibilité de bénéficier d'un **accès à distance** (flux bidirectionnel) **en temps réel**, d'initier **plusieurs communications simultanément** sur les serveurs et objets connectés, et cela **quel que soit le nombre d'objets associés**. Grâce à cela, la supervision et la maintenance à distance du parc (actions de mise à jour, paramétrage...) sont grandement simplifiées.

Guillaume Gimenez, gérant de la **société 2Gi Technologie**⁵ spécialisée dans l'informatique industrielle et client de Matooma atteste de la fiabilité de la solution MatooWan : « à l'époque, nous nous sommes posé la question de savoir si nous allions prendre des cartes SIM simples (sans infrastructure APN) ou une solution avec un APN. Nous n'avons pas voulu faire de développement interne et nous nous sommes tournés vers un acteur expérimenté dans le domaine du M2M, Matooma ».

Il ajoute : « nos principales priorités étaient la fiabilité et la sécurité. Chez d'autres fournisseurs d'APN, nous aurions eu trop de lacunes en matière de gestion de la fiabilité, et nous aurions dû faire face à des surconsommations importantes. La solution MatooWan nous a permis d'externaliser le maintien de notre infrastructure réseau opérateur en nous donnant la possibilité de réduire l'ensemble de nos coûts internes de fonctionnement ».

À propos de Matooma

Fondé en juin 2012 par son président Frédéric Salles et ayant rejoint le groupe Wireless Logic en juillet 2019, Matooma est un acteur expert dans la fourniture de cartes SIM et de services M2M/IoT industriels.

La société propose des offres sur mesure de connectivité multi-opérateur, de plateforme de gestion, et de sécurité à destination des fabricants d'objets, d'exploitants de services, d'intégrateurs et de distributeurs de solutions. Notre mission : aider nos clients dans le déploiement national et international de leurs projets IoT/M2M de façon simple, économique et rapide sans avoir recours à de multiples interlocuteurs.

Site web : www.matooma.com

⁵ Focus société 2Gi Technologie : créée en 2002 et spécialisée dans l'informatique industrielle, principalement dans le SCADA, l'IoT et le monitoring à distance. Pour plus d'informations rendez-vous sur : <http://2gitechnologie.com/>.