



IoT.

Quels outils pour quels usages ?

Les outils d'IoT (Internet of Things) sont plébiscités par un nombre croissant d'entreprises. Sans doute parce qu'ils sont riches de nombreux avantages pour celles-ci, en matière de sécurité comme de productivité. A condition, toutefois, de mettre en place les solutions répondant aux bons défis et de les piloter au quotidien. Dans cet ebook, découvrez tout ce que l'IoT peut apporter à votre entreprise !



01

Choisir les outils IoT adaptés à son SI : quelles solutions pour quelles pratiques ?

Pour les entreprises, mettre en place des outils d'IoT (Internet of Things/Internet des objets) peut présenter de nombreux avantages. A condition toutefois de faire appel à des solutions s'interfaçant bien avec le SI préexistant de l'entreprise, afin d'éviter de complexifier celui-ci.

Présentation des bonnes pratiques et des défis à relever, par Grégory Gatineau et Stéphane Leroux, respectivement Category Manager et Architecte solutions réseaux au sein de HPE Aruba Networking.

Lorsqu'une entreprise décide de mettre en place des outils IoT, comment s'y prendre ? Quels sont les outils incontournables ?

Grégory Gatineau. Ce dont il faut tout d'abord prendre conscience, c'est que nombre d'entreprises sont bicéphales ; par cela, j'entends que les équipes recourant au quotidien à l'IoT ne seront pas nécessairement celles qui auront la charge de la sécuriser. Les équipes métier vont donc parfois mettre en place des solutions répondant à leurs enjeux bien précis, mais déphasées par rapport aux exigences de cybersécurité. C'est là qu'est parfois le point d'achoppement, et c'est à cela que viennent répondre les solutions HPE Aruba Networking. Nos solutions intègrent donc directement du Wifi, du zigbee, du Bluetooth, des puces GPS ou des ports USB, afin d'étendre l'écosystème de connectivité au maximum et de garder de la visibilité sur tous les terminaux IoT – même lorsque ceux-ci font appel à des technologies différentes. Rapatrier ces flux sur le réseau Ethernet permet d'appliquer les mécaniques de cybersécurité déjà présentes. Nos solutions permettent également à nos clients d'entamer une réflexion sur l'évolution de leurs réseaux ; elles pourront interconnecter nos solutions avec leurs outils déjà en place, et simplifier le fonctionnement de ceux-ci tout en augmentant le niveau de sécurité global.

Stéphane Leroux. Effectivement, les entreprises ont logiquement un intérêt à mutualiser ces cas d'usages et leur sécurité sur un même réseau et au sein d'un seul outil de gestion, pour l'ensemble de leurs infrastructures. Cela incite donc les équipes à davantage de communication et de collaboration entre elles. Pourtant, une fois que l'on sait cela, comment piloter cet environnement convergé ? Nous exploiterons donc des technologies de segmentation dynamique, pour différencier les divers usages, via ce qu'on appelle les « rôles ». L'objectif est clairement de faire cohabiter et prioriser les flux, mais de façon silotée, étanche. Cela est d'autant plus aisé que l'un des avantages de l'IoT est qu'il est assez peu gourmand en bande passante.

Quels sont précisément les différents usages auxquels ces solutions IoT viendront répondre ?

Stéphane Leroux. En fonction de chaque secteur, il y aura bien sûr des spécificités. Je citerai toutefois un exemple que l'on retrouve dans de nombreux secteurs : le bâtiment intelligent, qui permet une gestion plus précise et rigoureuse de l'énergie. Ensuite, en fonction du secteur et des besoins clients, les solutions IoT seront davantage orientées. D'où l'importance pour HPE Aruba Networking de mettre en place un vaste écosystème, très diversifié – puisque nous ne pouvons proposer des solutions pleinement ciblées sur une activité particulière. Si l'on prend l'exemple du retail, les applications de l'IoT seront relatives à l'expérience client ou l'affichage des prix. Dans le secteur de la santé, il s'agira du parcours du patient ou du visiteur au sein d'un hôpital, ou encore le suivi des actifs. L'objectif, dans chaque cas de figure, est de faire qu'une infrastructure soit la plus ouverte possible, afin de couvrir un maximum d'usages – sans pour autant renoncer à la sécurité, ni complexifier l'infrastructure et le SI.

Quelle est la plus-value des solutions HPE Aruba Networking ?

Grégory Gatineau. Nous avons documenté un écosystème de partenaires technologiques, qui viendront fournir aux entreprises les solutions métier adaptés à leurs enjeux. Cet écosystème est développé et enrichi par une veille économique et technologique, qui a aussi lieu via nos clients et partenaires historiques. Il s'agit donc d'un processus continu ; parfois, il s'agit d'une solution identifiée par un de nos clients, et sur laquelle celui-ci vient nous demander conseil. Du fait de notre notoriété et de notre réputation, nous sommes également fréquemment contactés par des fournisseurs de solutions IoT souhaitant interfacer leur technologie avec la nôtre et s'ouvrir à de nouvelles perspectives. Nous pouvons donc jouer un vrai rôle de prescripteurs auprès de nos clients. Mais du fait que notre offre est ouverte par nature, via API, ARUBA peut interagir avec n'importe quelle solution pour peu qu'elle soit basée sur des standards industriels.

Cet aspect précis est primordial, surtout lorsque l'on sait qu'une infrastructure peut rester en place au sein d'une entreprise pendant 5, 10 voire parfois 15 ans ! Il faut donc être capable de se projeter dans le temps long, et que nos clients sachent qu'ils ont mis en place la bonne infrastructure, puisque c'est sur le bon fonctionnement de celle-ci que reposeront tous les enjeux IT et parfois métiers d'une entreprise. Mettre le bon réseau en place dès le départ, c'est le meilleur moyen de bien construire son SI ensuite.



02

Comment bien sécuriser et superviser ses équipements IoT ?

Les terminaux IoT pèsent un poids de plus en plus prépondérant dans le quotidien de nombreuses équipes métiers. Si ces pratiques émergentes sont porteuses de bien des bénéfices, elles doivent pourtant être suivies de près par la DSI afin de demeurer pleinement sécurisées. C'est la raison pour laquelle les équipes IT peuvent mettre en place des solutions spécialisées. Tour d'horizon avec Grégory Gatineau et Stéphane Leroux, respectivement Catégorie Manager et Architecte solutions réseaux au sein de HPE Aruba Networking.



Lorsqu'une entreprise a mis en place des outils d'IoT et qu'elle a pris ses dispositions concernant la bonne gestion de ceux-ci, il lui reste encore un chantier de taille : assurer la sécurité desdits outils IoT. Si la DSI de l'entreprise peut garder la mainmise sur de nombreuses opérations d'identification, celle-ci peut manquer de visibilité sur certains terminaux, comme ceux ayant trait au « shadow IT ». Grégory Gatineau précise : « Certaines équipes métier au

sein des entreprises sont dans une logique d'innovation permanente et cherchent à expérimenter, à tester des solutions qui pourraient les rendre plus compétitives ou efficaces. Si cela part souvent d'une bonne intention, la DSI n'a pas forcément donné son feu vert pour certains usages. Les équipes IT s'en rendent parfois compte trop tard, alors que le risque de sécurité est déjà avéré. »

Mieux communiquer pour mieux collaborer

Face à de telles évolutions sur le terrain, il est ainsi primordial que la DSI parvienne à conserver une visibilité complète sur tous les terminaux se connectant au réseau de l'entreprise, y compris les potentiels « éléments perturbateurs ». Ces pratiques qui émergent peuvent aussi être le point de départ d'une meilleure communication entre les équipes métiers et IT. Grégory Gatineau poursuit : « L'idée est d'ouvrir une discussion, de savoir selon quels paramètres configurer les outils, pour que chaque équipe en tire le meilleur parti sans créer de brèche de sécurité – et sans être non plus dans le blocage pur et simple. » Pour changer de paradigme en la matière, les entreprises doivent faire appel aux acteurs spécialisés, tels que HPE Aruba Networking afin d'avoir un large choix de solutions renforçant la sécurité des réseaux. Stéphane Leroux précise l'étendue des services fournis par HPE Aruba Networking en la matière : « Nos solutions permettent d'étendre les capacités de filtrage des pare-feux, lesquels sont directement intégrés aux équipements réseau. L'objectif derrière cela est de filtrer tous les flux, avant même que ceux-ci ne pénètrent au sein du réseau. »



L'idée est d'ouvrir une discussion, de savoir selon quels paramètres configurer les outils, pour que chaque équipe en tire le meilleur parti sans créer de brèche de sécurité – et sans être non plus dans le blocage pur et simple. »

Grégory Gatineau

Autre défi lié aux appareils IoT : la prolifération de ces équipements au sein des entreprises, qui complique de plus en plus leur sécurisation. A ce sujet, Grégory Gatineau explique : « D'une équipe à l'autre, il n'y a pas toujours de vraie standardisation sur les formats, la connectivité, les façons de communiquer... Tout ceci pose un réel problème pour la DSI, puisque celle-ci se retrouvera avec un véritable enchevêtrement de protocoles à mettre en place, de formats à faire cohabiter, de connexions à assurer. » C'est ici que les solutions HPE Aruba Networking entrent en jeu ; celles-ci permettront en effet de prendre en compte la totalité des éléments présents sur le réseau, sans pour autant que l'infrastructure s'en voit complexifiée. Cet outil jouera ici le rôle de « tiers de confiance » en vérifiant quel utilisateur cherche à se connecter, humain ou machine, à se documenter sur lui puis, le cas échéant, l'authentifier – en se portant garant de cette connexion et en continuant à vérifier tout au long de sa session d'utilisation au maintien de la cohérence de la politique de sécurité. Cela a un impact également sur l'écoresponsabilité de l'entreprise. Qui dit un seul réseau, dit également un seul câblage, et une seule fois la dépense énergétique pour en profiter.



Redonner davantage d'autonomie

Au-delà du gain évident de sécurité pour l'entreprise, cette solution permet également de redonner davantage d'autonomie aux équipes de terrain. Stéphane Leroux explique : « Si un équipement se déconnecte et se reconnecte à un autre endroit dans l'entreprise, il sera reconnu et sécurisé comme s'il n'avait jamais bougé. Je prendrai l'exemple trivial d'une imprimante : un collaborateur peut la débrancher au rez-de-chaussée et la connecter à un autre étage, en Wi-Fi ; celle-ci sera reconnue et accessible à tous les utilisateurs, sans qu'il y ait besoin de faire de demande à la DSI. Cette simplicité, nous sommes capables de la garantir à tout type d'équipements et IoT sur le réseau. Ce mécanisme fonctionnera tout aussi bien pour un IoT, une machine outils ou tout autre élément ayant été authentifié et autorisé par l'entreprise à profiter de son réseau »

Pour une entreprise, mettre en place les bons outils de sécurité est un bon moyen de rester à la pointe de l'innovation, mais aussi et surtout de conserver un réel avantage concurrentiel sur des marchés souvent compétitifs. Stéphane Leroux explique : « Une opération qui nécessitera peut-être plusieurs mois pour ses concurrents n'exigera que quelques semaines pour l'entreprise qui a mis en place nos solutions. Si on parle souvent de l'expérience utilisateur, il s'agira ici davantage de l'expérience administrateur, non moins capitale puisque la sécurité concerne toutes et tous au sein de l'entreprise. »



Si un équipement se déconnecte et se reconnecte à un autre endroit dans l'entreprise, il sera reconnu et sécurisé comme s'il n'avait jamais bougé. »

Stéphane Leroux



03

Comment garder la mainmise sur la gestion de ses appareils IoT ?

Lorsque les entreprises ont opté pour les outils d'IoT adaptés à leurs besoins et que ceux-ci ont été sécurisés, comment (bien) les piloter au quotidien ? Pour ce faire, les organisations peuvent se faire accompagner par des acteurs spécialisés tels que HPE Aruba Networking. Echange avec Grégory Gatineau et Stéphane Leroux, respectivement Catégorie Manager et Architecte solutions réseaux au sein de HPE Aruba Networking.



Pour une entreprise, garder la mainmise sur les différents terminaux IoT se connectant à son réseau est parfois difficile, alors que la multiplication des appareils IoT fait émerger de nouveaux défis pour les équipes IT. Pourtant, il est primordial qu'à tout moment les équipes IT sachent précisément quel appareil est connecté, et pour quel usage, ou encore ce qui fonctionne et ce qui dysfonctionne. Il est tout aussi essentiel que les entreprises aient à leur disposition des outils en mesure d'unifier les différents protocoles de communication et types de connectivité des outils IoT, qui nécessitent bien souvent des passerelles spécifiques afin de piloter les appareils et collecter les données. D'autant plus que les appareils ne sont pas fiables par nature et qu'un manque de visibilité peut générer des risques plus importants pour l'entreprise. De fait, l'intégration des données IoT aux processus métier est complexe et nécessite des connaissances approfondies en IoT et leur intégration. Les équipes IT, sollicitées sur un vaste nombre de sujets, doivent donc bien s'entourer.

Des recommandations simples à mettre en pratique

Pour accompagner les organisations dans la gestion de leurs ressources IoT, les acteurs spécialisés n'ont cessé de faire évoluer leurs solutions, notamment en y intégrant de l'intelligence artificielle. En effet, les dernières technologies développées sont en mesure de le faire précisément, mais aussi de faire des recommandations de maintenance prédictive à l'administrateur du réseau, lesquelles peuvent être mis en pratique simplement par les entreprises. Grégory Gatineau explique : « L'administrateur d'un SI sur lequel les solutions HPE Aruba Networking sont déployées consulte son interface, sur laquelle un smiley rouge apparaît en cas d'alerte ; il peut s'agir d'un appareil IoT qui ne fonctionne pas. L'administrateur demandera à l'IA « d'enquêter » et prendre ensuite une décision éclairée par la télémétrie que remonte le réseau physique. »



L'administrateur d'un SI sur lequel les solutions HPE Aruba Networking sont déployées consulte son interface, sur laquelle un smiley rouge apparaît en cas d'alerte ; il peut s'agir d'un appareil IoT qui ne fonctionne pas.»

Grégory Gatineau



Les points d'accès extensibles Wi-Fi 6, Wi-Fi 6E et Wi-Fi 7 de HPE Aruba Networking prennent en charge de nombreuses technologies IoT ; les entreprises peuvent donc gérer une large gamme d'applications IoT avec leur infrastructure HPE Aruba Networking déjà en place, et ainsi éliminer le coût, la complexité et les vulnérabilités potentielles des passerelles et réseaux IoT superposés. De plus, les entreprises peuvent appliquer les principes de sécurité Zero Trust : la segmentation dynamique automatise l'identification des appareils, l'application des politiques et leur mise en œuvre, et facilite l'évolutivité de l'adoption de l'IoT.

“

Une solution qui permet d'émettre des diagnostics et d'effectuer des dépannages, fait gagner du temps à chaque maillon de la chaîne, et améliore donc l'expérience – que cela soit celle de l'opérateur ou de l'utilisateur. »

Stéphane Leroux

Faire gagner du temps à chaque maillon de la chaîne

Pour un DSI devant souvent gérer des parcs étendus avec des équipes réduites, pouvoir automatiser de nombreuses tâches et accélérer la prise de décision représente ainsi un apport inestimable. Ces solutions peuvent être aisément paramétrées au sein d'écosystèmes existants et interagir avec les outils existants, pour assurer une connexion et une sécurisation optimales. Selon Stéphane Leroux, mettre en place les bons outils est aussi riche de nombreux autres avantages : « Une solution qui permet d'émettre des diagnostics et d'effectuer des dépannages, fait gagner du temps à chaque maillon de la chaîne, et améliore donc l'expérience – que cela soit celle de l'opérateur ou de l'utilisateur. L'IA s'enrichit d'autant plus qu'elle a accès à un très grand nombre de données stockées dans le cloud, cela enrichi l'intelligence de nos plateformes, du fait du fonctionnement en crowdsourcing. »

Même les entreprises qui ne souhaitent pas rester dépendantes du cloud pourront développer des solutions IoT fonctionnant en vase clos, en demeurant tout aussi flexible et tirer pleinement parti de l'IA. Grégory Gatineau précise : « On pense souvent au cloud lorsque l'on entend parler d'IoT mais il ne va pas de soi dans certains secteurs. Pour certains d'entre eux, c'est même dans le cahier des charges de ne pas embarquer du cloud, notamment dans certaines entités publiques, par exemple rattachées à l'armée. »



**Quelle que soit leur taille
ou leur secteur d'activité,
les entreprises pourront trouver
une solution IoT HPE Aruba Networking
à la hauteur de leur défi,
et la déployer en étant accompagnées
par des équipes spécialisées.**