Chapitre 2 .Architectures IoT

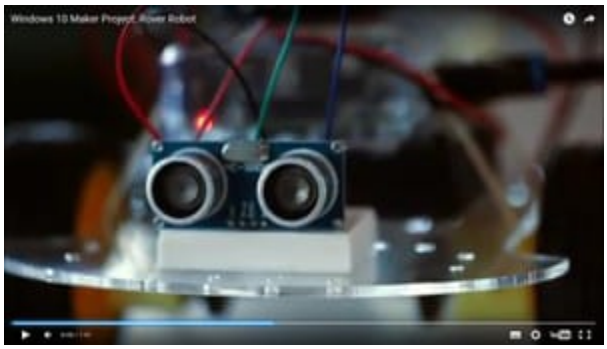
Introduction :

Disposant par définition de peu de ressources, les objets connectés requièrent des OS légers et orientés temps réel. Microsoft, Google ou encore Intel se positionnent sur le créneau.

A première vue, il y a peu de points communs entre une montre connectée, un bracelet d'automesure et un capteur de chaleur. Ces objets connectés ont toutefois des contraintes identiques. Ils disposent par définition de peu de ressources, doivent être optimisés en matière de consommation d'énergie, et être à même d'échanger des données en temps réel avec le monde extérieur. Il suppose donc un système d'exploitation à la fois frugal et à même de supporter un grand nombre d'architectures (x86, MIPS, ARM…) et de protocoles communication (Bluetooth, 6LoWPAN…).

A la quête de l'OS idéal

Depuis une quinzaine d'années, on assiste à une multiplication de ces "Real Time OS" (RTO), pouvant fonctionner à partir de quelques KB de RAM. Historiquement, ces RTOS viennent du monde open source et sont avant tout dévolus aux systèmes embarqués à l'image de FreeRTOS ou Contiki.



Robot de démonstration motorisé par Windows 10 IoT Core. Il a été construit par les équipes Microsoft. © Capture vidéo / JDN

Ce domaine des RTO a été récemment rejoint par de grands noms de l'informatique. En rachetant Wind River, Intel a acquis les solutions logicielles du même nom qu'il a adaptées au monde de l'internet des objets. Son concurrent direct, ARM a développé mbed OS, un système d'exploitation au service de ses microcontrôleurs à cœur Cortex-M.Les fabricants de semi-conducteurs ne sont pas les seuls dans cette quête de l'OS poids plume. Dans sa volonté de diffuser Windows 10 sur l'ensemble des terminaux, Microsoft a dévoilé cet été un système dédié : Windows 10 IoT Core. De son côté, Google veut, avec Brillo, renouveler le succès d'Android dans le monde des objets connectés.

Même si ces nouveaux OS sont gratuits et le plus souvent open source, Christian Charreyre, associé au cabinet CIO Systèmes Embarqués, ne peut s'empêcher de faire une distinction entre "les systèmes qui relèvent des communautés du libre et ceux d'acteurs à vocation commerciale".

L'un des avantages, à ses yeux, des OS open source, c'est leur capacité, de par leur ancienneté, à supporter un grand nombre de plateformes matérielles. Car après avoir trouvé l'OS idéal, il

faut s'assurer de sa portabilité dans son environnement d'accueil. "Plus un OS est vieux et plus il dispose de BSP, ces Boarding support package qui font le pont entre l'OS et le hardware. C'est l'équivalent du Bios dans le monde du PC", explique l'expert. Autre critère de choix, l'adhésion à Posix, le standard qui définit les interfaces communes aux systèmes de type Unix.

Google ou Microsoft rattrapent cette lacune en multipliant les partenariats avec des fabricants

plus jeunes sur ce marché des RTOS, Google ou Microsoft rattrapent cette lacune en multipliant les partenariats avec des fabricants de cartes de développement comme Qualcomm, Intel ou Freescale. Ils peuvent mettre aussi en action leur formidable force de frappe pour promouvoir leurs outils tout en les intégrant à l'ensemble de leur offre, notamment pour la partie collecte et analyse des données dans le cloud.Le public visé diffère aussi. Alors que les OS open source se retrouvent dans un grand nombre d'applications industrielles, les grands noms de l'IT font le pari d'ouvrir le marché au grand public, lorgnant particulièrement la communauté des " makers ". De fait, ces nouveaux OS sont plus gourmands en espace mémoire (on parle de Mo) et en taille de processeurs (32 ou 64 bits).

Windows 10 IoT Core : Microsoft fait de l'œil aux "makers"

Microsoft n'a pas perdu de temps. Un mois après la sortie officielle de Windows 10, l'éditeur annonçait, en août 2015, une version de son système d'exploitation dédiée aux objets connectés. Visant avant tout la communauté des "makers", Windows 10 IoT Core est un OS allégé en téléchargement gratuit, qui supporte des cartes mères comme Raspberry Pi 2, MinnowBoard Max (Intel) ou DragonBoard 410c (Qualcomm).

Windows 10 IoT Core intègre C ++, C #, JavaScript ou Visual Basic

Concevoir des objets connectés à base de Raspberry Pi 2

Microsoft s'est même associé à Adafruit pour commercialiser un pack de démarrage comprenant tous les éléments nécessaires pour concevoir un objet connecté à base de Raspberry Pi 2 - avec notamment des capteurs d'humidité et de température.Pour favoriser l'adoption de son OS orienté IoT, Microsoft a donné des gages aux développeurs. Windows 10 IoT Core intègre des langages standard comme C ++, C #, JavaScript ou Visual Basic mais aussi Node.js (y compris Node.js Express) et Python. Sous un environnement Windows 10, il faut toutefois disposer de Visual Studio 2015.

Dans les dernières versions de Windows 10 IoT Core, la connectivité a été renforcée avec le support du Wi-fi et de Bluetooth. Du côté du traitement de données de masse issues des objets connectés, Microsoft peut mettre en avant l'offre Azure IoT Suite de son cloud maison, lancée en version finale en septembre.

Windows 10 IoT Core en bref	
Points forts	Points faibles
- Les partenariats avec les	- La jeunesse du système

Windows 10 IoT Core en bref	
Points forts	Points faibles
fabricants de cartes mères - Le nombre de langages supportés - L'intégration au cloud Azure	d'exploitation - Son positionnement marqué à destination des "makers"

Wind River Rocket : la puissance de feu d'Intel

Brique par Brique, Intel bâtit sa plateforme dédiée à l'internet des objets. En novembre 2015, le fabricant de semiconducteurs a annoncé trois nouveaux processeurs de sa gamme de Quark (SE, D1000 et D2000) spécialement dessinés pour les microcontrôleurs à basse consommation. Sur ce terrain, le fondeur s'appuie aussi sur l'offre logicielle de Wind River, éditeur racheté en 2009.

A son portefeuille, Intel propose deux OS qui couvrent le spectre. Wind River Rocket est un système d'exploitation temps réel conçu pour les applications s'exécutant sur des microcontrôleurs 32 bits - en environnements Intel x86 mais aussi ARM. Gratuit, il vise le marché des capteurs ou des dispositifs d'automesure (*quantified self*). Côté hardware, Wind River Rocket supporte la carte de développement d'Intel Galileo Gen 2. Le support de la carte Freedom-K64F de Freescale sera prochainement disponible. La documentation et la bibliothèque de codes sont publiées sur Github.

Le second système d'exploitation, Wind River Pulsar, est un OS Linux taillé pour les différents types de processeur, des microcontrôleurs 32 bits jusqu'aux microprocesseurs 64 bits. Ces deux OS sont intégrés dans la suite logicielle en mode SaaS Wind River Helix, une plateforme de développement d'applications mais aussi de collecte et d'analyse des données.

Wind River Rocket en bref	
Points forts	Points faibles
- La capacité d'Intel à couvrir toute la filière IoT : processeurs, cartes, OS... - L'intégration à la plateforme de développement cloud Helix	- La jeunesse du système d'exploitation - La taille des processeurs exigée (32 ou 64 bit)

Google Brillo capitalise sur la force d'Android

En mai, lors de son dernier événement Google I/O, Google dévoilait l'existence de Brillo, son OS dédié à l'internet des objets. Depuis, les développeurs sont invités à s'inscrire en ligne pour faire partie du programme. Basé sur Android, cet OS allégé sera associé à Weave, la plateforme

de communication de Google pour les objets connectés, utilisée notamment pour les produits Nest. Google fait toutefois savoir que Weave peut fonctionner avec un OS basé sur Linux tandis que Brillo intègre, de son côté, le Wi-fi et Bluetooth. Brillo vise à la fois les développeurs d'applications, la communauté des "makers" et les fabricants OEM. Avec un penchant affirmé pour la domotique afin visiblement de concurrencer Apple et son HomeKit présenté un an plus tôt. A l'instar d'Android, Brillo supporte les architectures d'Intel (x86), de MIPS ou d'ARM. Des développements spécifiques ont été faits autour de Brillo pour la carte Dragonboard 410c de Qualcomm et l'ordinateur ultra compact Edison d'Intel. Imagination Technologies a fait aussi savoir que sa dernière carte de développement, baptisée Creator Ci40, était compatible Brillo. Autre concrétisation de Brillo, Google a commercialisé aux Etats-Unis, en partenariat avec les constructeurs TP-Link et Asus, OnHub, un routeur qui gère intelligemment le Wi-fi dans les différentes pièces d'une maison.

Google Brillo en bref	
Points forts	Points faibles
- Le support d'un grand nombre d'architectures (x86, MIPS, ARM) - Les partenariats avec les fabricants de cartes	- La jeunesse du système d'exploitation - La dépendance à Weave, la plate de communication de Google

FreeRTOS, l’ancêtre des OS temps réel

FreeRTOS préexistait bien avant la vague des objets connectés puisqu'il a été créé en 2003. Disponible sous licence GPL, cet OS open source pour microcontrôleurs et petits micro-processeurs est l'un des systèmes d'exploitation les plus utilisés dans le monde de l'embarqué.Conçu pour être très léger (il pèse de 6 Ko à 12 Ko), le noyau de l'OS n'est composé que de trois fichiers source écrits en langage C. FreeRTOS se destine donc aux systèmes embarqués ayant peu d'espace mémoire tout en devant gérer les contraintes du temps réel. Il sert souvent de base pour le développement d'applications propriétaires dans des domaines aussi variés que l'automobile ou le médical.

Pour l'ouvrir justement au monde de l'IoT, Real Time Engineers, une société britannique qui développe et maintient FreeRTOS s'est rapprochée du danois Nabto qui développe, lui, une plateforme de communication temps réel. Ensemble, ils ont packagé une offre payante baptisée FreeRTOS+Nabto. Natbo apportant à l'OS une connectivité IP bas débit et un cryptage des données.

FreeRTOS en bref	
Points forts	Points faibles
- L'ancienneté du système	- Un OS pas spécifiquement

FreeRTOS en bref	
Points forts	Points faibles
d'exploitation, sa diffusion - Le nombre de hardwares supportés	dédié IoT - Une prise en main qui peut s'avérer complexe

OpenEmbedded, un framework issu du monde de l'embarqué :

Comme FreeRTOS, OpenEmbedded est issu du monde de l'embarqué. Conçu lui aussi en 2003, il s'agit d'un framework basé sur Linux qui sert à automatiser la compilation de composants destinés à être ensuite déployés sur des systèmes embarqués. Basé sur le moteur BitBake (qui est écrit en Python), OpenEmbedded propose un jeu de recettes pour fabriquer les paquets logiciels.

Sa prise en main n'étant pas aisée, OpenEmbedded fait depuis mars 2011 partie intégrante du projet Yocto mis en place par la Linux Fondation et soutenu par un certain nombre de fournisseurs - dont Intel et Texas Instruments. Le projet Yocto vise à simplifier la génération de distributions GNU/Linux embarqué à partir du code source original d'OpenEmbedded. Des distributions générées à partir de Yocto sont compatibles pour les architectures x86, ARM, MIPS et IBM PowerPC. Un certain nombre de dispositifs matériels sont supportées notamment la carte BeagleBoard de Texas Instruments.

OpenEmbedded en bref	
Points forts	Points faibles
- L'ancienneté du système d'exploitation - Sa compatibilité avec un grand nombre d'architectures (x86, ARM, MIPS et PowerPC)	- Prise en main délicate - Son positionnement qui le destine spécifiquement aux gateways

Contiki, l'OS star des capteurs sans fil

Créé en 2004 par une équipe de chercheurs suédois. Contiki est un système d'exploitation dédié avant tout aux mini-capteurs sans fil. Il permet de les faire dialoguer avec n'importe quel matériel supportant le protocole IP, y compris IPv6. Constitué d'un ordonnanceur et d'un jeu de processus, Contiki occupe peu d'espace mémoire - moins de 10 Ko de RAM et 30 Ko de ROM - pour une consommation électrique très faible.Publié sous licence BSD (qui permet de réutiliser tout ou une partie du code source sans restriction), Contiki est écrit en C, ce qui lui assure une meilleure portabilité que d'autres OS légers qui lui sont

traditionnellement comparés comme TinyOS ou LiteOS. Il propose un environnement de développement simplifié, nommé Instant Contiki. Se présentant sous la forme d'une machine virtuelle VMware, il contient tout le code source de Contiki accompagné du simulateur Cooja.

Une nouvelle version a été annoncée cet été sur le blog officiel. Cette 3.0 supporte désormais la plate-forme SensiorTag de Texas Instruments, grâce à la prise en compte des protocoles de communication sans fil Bluetooth et 6LoWPAN. Contiki devient également compatible avec Re-Mote de Zolertia, un module de développement qui permet de communiquer sur de longues distances. Il est notamment utilisé pour les projets de villes intelligentes (smart cities).

Contiki en bref	
Points forts	Points faibles
- Environnement de développement simplifié à partir d'une machine virtuelle - La prise en compte de Bluetooth et 6LoWPAN dans la version 3.0	- Son positionnement sur les mini-capteurs sans fil

RIOT, un nouveau-né franco-allemand : RIOT est l'un des derniers nés des OS open source puisqu'il a été rendu public en 2013. La communauté qui le développe est activement soutenue par la recherche académique - notamment par l'Inria en France et les universités de Berlin et Hambourg en Allemagne. Comme son nom l'indique - R (pour "real time") et IOT (pour "internet of things") - RIOT est spécifiquement dédié aux objets connectés. Issu du projet FeuerWare, lui-même inspiré de Contiki, RIOT ambitionne de connecter une très large gamme de microcontrôleurs ou de processeurs quelle que soit l'architectures système, du 16 au 32 bits. Son empreinte mémoire est particulièrement faible : environ 1,5 Ko en mémoire Ram et 5 Ko en Rom. Disponible sous licence LGPLv2, RIOT utilise les langages de programmation C et C++ tout en étant partiellement compatible avec Posix. Ses promoteurs mettent aussi en avant ses capacités de traitement temps réel, son efficacité énergétique et sa connectivité réseau (IPv6, 6LoWPAN, RPL et UDP).

RIOT en bref	
Points forts	Points faibles
- L'étendu des langages de programmation pris en charge (C, C++), la compatibilité partielle à Posix - La connectivité réseau	- La jeunesse du système d'exploitation - Le manque de supports hardware

Comparatif des OS orientés IoT : tableau de synthèse

Comparatif des OS orientés **IoT** : tableau de synthèse				
OS	**Empreinte mémoire**	**Langages**	**Connectivité réseau**	**Compatibilité matérielle**
Windows 10 IoT Core	128 MB de Ram minimum	C ++, C #, JavaScript, Visual Basic, Node.js et Python	Wi-fi et Bluetooth	Partenariats Raspberry, Intel, Qualcomm.
Intel Wind River	A partir de 4 KB de Ram	NC	Wi-fi, Bluetooth, ZigBee	Architectures Intel x86 et ARM
Google Brillo	32 MB minimum de Ram et 128 MB de Rom	Base Android	Weave, wi-fi, Bluetooth	Architectures x86, MIPS, ARM. Partenariats Intel et Qualcomm
FreeRTOS	6 à 12 KB de Ram, 5 à 10 KB de Rom	C	Connectivité IP avec l'apport de Nabto	Plus d'une quarantaine d'architectures supportées
OpenEmbedded	Au minimum quelques dizaines de MB de Ram et de 32 à 64 MB de Rom	C, C++, Perl, Python, Java, Mono	Bluetooth, 6LoWPAN	Architectures x86, ARM, MIPS et IBM PowerPC
Contiki	Moins de 2 KB de Ram et moins de 30 KB de Rom	C	Bluetooth, 6LoWPAN	Partenariats avec Texas Instruments, et Zolertia
RIOT	Environ 1,5 KB de Ram et 5 KB de Rom	C, C++	IPv6, 6LoWPAN, RPL et UDP	NC

Types de Cloud Computing – un guide complet sur les solutions et technologies de Cloud en 2021

Aujourd'hui, le Cloud Computing est devenu une technologie courante, avec de nombreux types
de Cloud Computing . Selon le dernier rapport « State of Cloud », on estime que 94 % des entreprises utilisent au moins un service de Cloud Computing.Et pourtant, la capacité de croissance du Cloud reste exponentielle, une étude commandée par IBM faisant état de seulement 20 % des charges de travail des entreprises fonctionnant actuellement dans le Cloud. N'ayant migré que les charges de travail les plus simples, les entreprises ont encore un long chemin à parcourir dans le Cloud. Avec 80 % des charges de travail des entreprises fonctionnant encore sur site, leur migration représenterait un quadruplement potentiel du marché actuel du Cloud.

Malgré la maturité du marché du Cloud, de nombreuses organisations ne connaissent pas encore les services et les modèles de déploiement disponibles. De nouveaux produits et services de Cloud Computing arrivent presque chaque jour, grâce à l'innovation constante des leaders technologiques comme Google, Amazon et Microsoft.

Quels sont les principaux types de Cloud Computing ?

Au plus haut niveau, le Cloud Computing est fourni par une combinaison de modèles de service et de déploiement. Dans chacun de ces modèles, il existe trois types de Cloud Computing et d'offres de services (aaS) parmi lesquels choisir.

Modèles de services de Cloud Computing : Il existe trois principaux modèles de services de Cloud Computing : l'infrastructure en tant que service, la plate-forme en tant que service et le logiciel en tant que service. Chaque modèle de service représente une partie différente du Cloud Computing et comprend sa propre division unique des responsabilités entre vous et le fournisseur de services.

Infrastructure as a service (IaaS) : c'est le modèle de service qui constitue la base du déploiement de votre technologie dans le Cloud. Grâce à un fournisseur IaaS, vous bénéficiez d'un accès à la demande via Internet aux ressources informatiques de base, notamment les ordinateurs (matériel virtuel ou dédié), la mise en réseau et le stockage.

L'IaaS vous donne accès à une ressource matérielle flexible et de pointe qui peut être adaptée aux besoins de traitement et de stockage de votre entreprise. Vous utilisez cette infrastructure pour fournir les applications, les logiciels et les plateformes de votre organisation, sans avoir à en assurer la gestion et la maintenance.

Plateform as a service (PaaS):c' est le modèle de service de Cloud dans lequel vous accédez à des outils matériels et logiciels combinés par l'intermédiaire d'un fournisseur de services. Le PaaS est le plus souvent utilisé pour le développement d'applications.

Un fournisseur PaaS vous donne accès à l'infrastructure combinée de Cloud nécessaire au développement d'applications – bases de données, intergiciels, systèmes d'exploitation, serveurs – sans la complexité sous-jacente de sa gestion. Cela vous permet de devenir plus efficace. Au lieu de passer du temps à installer et à configurer l'infrastructure, vous vous concentrez uniquement sur le développement, l'exécution et la gestion des applications.

Software as a service (SaaS) : c'est le modèle de service de Cloud qui vous permet d'accéder à un produit logiciel complet, exécuté et géré par le fournisseur de services. La plupart des solutions SaaS ont tendance à être des applications destinées à l'utilisateur final.

L'accès au logiciel de votre choix à l'aide d'un modèle SaaS vous permet de vous concentrer uniquement sur la meilleure façon d'utiliser ce logiciel. Le fournisseur SaaS est responsable de la fourniture, de la maintenance et de la mise à jour du logiciel, y compris de l'infrastructure sous-jacente.

Modèles de déploiement du Cloud Computing

Une fois que vous avez sélectionné le ou les services de Cloud Computing que vous avez choisi, vous avez le choix entre trois principaux modèles de déploiement de Cloud Computing : le Cloud public, le Cloud privé et le Cloud hybride.

Comment fonctionne la sécurité dans le Cloud ?

La sécurité dans le Cloud est une interaction complexe de technologies, de contrôles, de processus et de politiques. Une pratique qui est hautement personnalisée en fonction des exigences uniques de votre organisation.Il n'existe donc pas d'explication unique qui englobe le « fonctionnement » de la sécurité dans le Cloud.

A Model for Securing Cloud Workloads (Image source: HyTrust)

Heureusement, il existe un ensemble de stratégies et d'outils largement établis que vous pouvez utiliser pour mettre en place une solide sécurité dans le Cloud.

Gestion des identités et des accès : Toutes les entreprises doivent disposer d'un système de gestion des identités et des accès (IAM) pour contrôler l'accès aux informations. Votre fournisseur de cloud computing s'intégrera directement à votre IAM ou proposera son propre système intégré. Un IAM combine des politiques d'authentification et d'accès des utilisateurs à plusieurs facteurs, vous aidant à contrôler qui a accès à vos applications et à vos données, ce à quoi ils peuvent accéder et ce qu'ils peuvent faire à vos données.

Sécurité physique:est un autre pilier de la sécurité dans le Cloud. Il s'agit d'une combinaison de mesures visant à empêcher l'accès direct et la perturbation du matériel hébergé dans le centre de données de votre fournisseur de cloud computing. La sécurité physique comprend le contrôle de l'accès direct par des portes de sécurité, une alimentation électrique ininterrompue, la vidéo en circuit fermé, des alarmes, le filtrage de l'air et des particules, la protection contre les incendies, etc.

Renseignement, surveillance et prévention des menaces : Le renseignement sur les menaces, les systèmes de détection d'intrusion (IDS), et les systèmes de prévention des intrusions (IPS) constituent l'épine dorsale de la sécurité dans le Cloud. Les outils de renseignement sur les menaces et les IDS offrent des fonctionnalités pour identifier les attaquants qui ciblent actuellement vos systèmes ou qui

constitueront une menace future. Les outils IPS mettent en œuvre des fonctionnalités permettant d'atténuer une attaque et de vous avertir de sa survenance afin que vous puissiez également y répondre.

Cryptage : En utilisant la technologie du Cloud, vous envoyez des données vers et depuis la plateforme du fournisseur de Cloud, souvent en les stockant dans leur infrastructure. Le cryptage est une autre couche de la sécurité dans le Cloud pour protéger vos données, en les encodant lorsqu'elles sont au repos et en transit. Cela garantit que les données sont quasiment impossibles à déchiffrer sans une clé de décryptage à laquelle vous seul avez accès.

Test de vulnérabilité et de pénétration du Cloud : Une autre pratique pour maintenir et améliorer la sécurité dans le Cloud est des tests de vulnérabilité et de pénétration. Ces pratiques impliquent que vous – ou votre fournisseur – attaquiez votre propre infrastructure de Cloud afin d'identifier toute faiblesse ou exploitation potentielle. Vous pouvez ensuite mettre en œuvre des solutions pour corriger ces vulnérabilités et améliorer votre position en matière de sécurité.

Micro-Segmentation :est de plus en plus courante dans la mise en œuvre de la sécurité dans le Cloud. Il s'agit de la pratique consistant à diviser votre déploiement dans le Cloud en segments de sécurité distincts, jusqu'au niveau de la charge de travail individuelle.

En isolant les charges de travail individuelles, vous pouvez appliquer des politiques de sécurité flexibles pour minimiser les dommages qu'un attaquant pourrait causer, s'il y avait accès.

Pare-feu de nouvelle génération : sont une autre pièce du puzzle de la sécurité dans le Cloud. Ils protègent vos charges de travail en utilisant les fonctionnalités traditionnelles des pare-feux et des fonctionnalités avancées plus récentes. La protection traditionnelle du pare-feu comprend le filtrage de paquets, l'inspection d'état, le proxy, le blocage d'IP, le blocage de noms de domaine et le blocage de ports.

Les pare-feu de nouvelle génération ajoutent un système de prévention des intrusions, une inspection approfondie des paquets, un contrôle des applications et une analyse du trafic crypté pour assurer une détection et une prévention complètes des menaces.

Remarque :La sécurité est une préoccupation pour toutes les entreprises qui, si c'est négligé, peut avoir un impact significatif sur la réputation et les résultats. Découvrez les 7 risques de sécurité du cloud computing

7 Risques de sécurité du cloud computing : Que vous opériez ou non dans le Cloud, la sécurité est une préoccupation pour toutes les entreprises. Vous serez confronté à des risques tels que le déni de service, les logiciels malveillants, L'injection SQL, les violations de données et les pertes de données. Tous ces éléments peuvent avoir un impact significatif sur la réputation et les résultats de votre entreprise.

Lorsque vous passez au Cloud, vous introduisez un nouvel ensemble de risques et changez la nature des autres. Cela ne signifie pas que le cloud computing n'est pas sécurisée. En fait, de nombreux fournisseurs de cloud computing offrent un accès à des outils et des ressources de sécurité très sophistiqués auxquels vous ne pourriez pas accéder autrement.

Cela signifie simplement que vous devez être conscient de l'évolution des risques afin de les atténuer. Examinons donc les risques de sécurité propres au cloud computing.

1. **Perte de visibilité :**La plupart des entreprises accèdent à une gamme de services de Cloud par l'intermédiaire de plusieurs appareils, services et géographies. Ce type de complexité dans une installation de cloud computing – sans les outils appropriés en place – peut vous faire perdre la visibilité de l'accès à votre infrastructure.Sans les processus appropriés en place, vous pouvez perdre de vue qui utilise vos services en ligne. Y compris les données auxquelles ils accèdent, qu'ils téléversent et téléchargent.

Si vous ne pouvez pas le voir, vous ne pouvez pas le protéger. Ce qui augmente le risque de violation et de perte de données.

2. **Violations de conformité :**Avec l'augmentation du contrôle réglementaire, vous devrez probablement respecter une série d'exigences de conformité strictes. En passant au Cloud, vous introduisez le risque des violations de conformité si vous ne faites pas attention.Nombre de ces réglementations exigent que votre entreprise sache où se trouvent vos données, qui y a accès, comment elles sont traitées et comment elles sont protégées. D'autres réglementations exigent que votre fournisseur de services de Cloud détienne certaines références de conformité.Un transfert négligent de données vers le cloud, ou un transfert vers le mauvais fournisseur, peut mettre votre organisation dans un état de non-conformité. Cela peut avoir de graves répercussions juridiques et financières.

3. **Absence de stratégie et d'architecture de sécurité du Cloud :**Il s'agit d'un risque de sécurité dans le Cloud que vous pouvez facilement éviter, mais que beaucoup n'ont pas. Dans leur hâte de migrer les systèmes et les données vers le cloud, de nombreuses organisations deviennent opérationnelles bien avant que les systèmes et les stratégies de sécurité ne soient en place pour protéger leur infrastructure.

Ici, chez Kinsta, nous comprenons l'importance d'un état d'esprit axé sur la sécurité lors du passage au cloud. C'est pourquoi Kinsta fournit des migrations WordPress gratuites pour assurer que votre transition vers le cloud est à la fois sécurisée et évite les temps d'arrêt prolongés.

Veillez à mettre en place une stratégie et une infrastructure de sécurité conçues pour que le cloud soit aligné avec vos systèmes et vos données.

4. **Menaces d'initiés :**Vos employés, entrepreneurs et partenaires commerciaux de confiance peuvent constituer certains de vos plus grands risques en matière de

sécurité. Ces menaces internes ne doivent pas nécessairement avoir une intention malveillante pour causer des dommages à votre entreprise. En fait, la majorité des incidents d'initiés sont dus à un manque de formation ou à une négligence.

Bien que vous soyez actuellement confronté à ce problème, le passage au cloud change le risque. Vous contrôlez vos données à votre fournisseur de services de Cloud et introduisez une nouvelle couche de menace interne de la part des employés du fournisseur.

5. **Violations contractuelles :**Tout partenariat contractuel que vous aurez établi comportera des restrictions sur l'utilisation des données partagées, leur stockage et les personnes autorisées à y accéder. Vos employés qui déplacent involontairement des données restreintes dans un service de Cloud sans autorisation pourraient créer une rupture de contrat qui pourrait entraîner des poursuites judiciaires.

Assurez-vous de lire les conditions générales de vos fournisseurs de services de Cloud. Même si vous avez l'autorisation de transférer des données vers le cloud, certains fournisseurs de services incluent le droit de partager toute donnée téléversée dans leur infrastructure. Par ignorance, vous pourriez involontairement violer un accord de non-divulgation.

6. **Interface utilisateur d'application non sécurisée (API) :**Lorsque vous utilisez des systèmes d'exploitation dans une infrastructure de Cloud, vous pouvez utiliser une API pour mettre en œuvre le contrôle. Toute API intégrée dans vos applications web ou mobiles peut offrir un accès en interne au personnel ou en externe aux consommateurs. Ce sont les API orientées vers l'extérieur qui peuvent introduire un risque de sécurité dans le Cloud. Toute API externe non sécurisée est une passerelle offrant un accès non autorisé aux cybercriminels qui cherchent à voler des données et à manipuler des services.

L'exemple le plus marquant d'une API externe non sécurisée est le Scandale de Cambridge Analytica de Facebook. L'API externe non sécurisée de Facebook a permis à Cambridge Analytica d'accéder aux données des utilisateurs de Facebook.

7. **Mauvaise configuration des services de Cloud :**La mauvaise configuration des services de Cloud est un autre risque potentiel pour la sécurité du Cloud. Avec la gamme et la complexité croissantes des services, ce problème prend de l'ampleur. Une mauvaise configuration des services de Cloud peut entraîner l'exposition publique, la manipulation ou même la suppression de données.

Parmi les causes communes, citons la conservation des réglages de sécurité et de gestion de l'accès par défaut pour les données hautement sensibles. D'autres incluent une gestion d'accès mal adaptée donnant accès à des personnes non autorisées, et un accès aux données mutilées où les données confidentielles sont laissées ouvertes sans autorisation.

Pourquoi la sécurité du Cloud est nécessaire :L'adoption massive de la technologie de Cloud, combinée à un volume et à une sophistication toujours plus grands des cyber-menaces, est à l'origine du besoin de sécurité dans le Cloud. Si l'on réfléchit aux risques de sécurité liés à l'adoption de la technologie dans le Cloud – décrits ci-dessus – l'incapacité à les atténuer peut avoir des conséquences importantes.

Mais tout n'est pas négatif, la sécurité dans le Cloud peut aussi offrir des avantages importants. Examinons pourquoi la sécurité dans le Cloud est une exigence essentielle.

Les menaces pour la cybersécurité continuent de s'accroître :L'une des forces motrices des pratiques sécurisées dans le Cloud est la menace toujours croissante des cybercriminels, tant en volume qu'en sophistication. Pour quantifier cette menace, un rapport sur la sécurité du cloud de l'ISC2 a révélé que 28 % des entreprises ont connu un incident de sécurité du cloud en 2019. Avec le gouvernement britannique signalant également que 32 % des entreprises britanniques ont subi une attaque sur les systèmes au cours des 12 derniers mois.

Prévention des violations et des pertes de données : Une conséquence de ces cyber-menaces accrues est l'accélération de la fréquence et du volume des violations et des pertes de données. Rien qu'au cours des six premiers mois de 2019, le rapport sur les menaces émergentes de Norton a souligné que plus de 4 milliards d'enregistrements ont été violés.

Une perte ou une violation de données peut avoir des implications juridiques, financières et de réputation importantes. IBM estime maintenant le coût moyen d'une violation de données à 3,92 millions de dollars US dans son dernier rapport.

Éviter les violations de conformité : Nous avons déjà mentionné comment la sécurité dans le Cloud comporte le risque de violations de la conformité. Pour démontrer les implications de la non-conformité, il suffit d'observer l'organisme fédéral allemand de surveillance de la vie privée qui a récemment infligé à 1&1 Telecommunications une amende de 9,55 millions d'euros pour violation du règlement général de l'UE sur la protection des données (RGPD).

Maintenir la continuité des activités : Une bonne sécurité dans le Cloud contribue à maintenir la continuité de vos activités. La protection contre les menaces telles que les attaques par déni de service (DDoS). Les interruptions de service imprévues et les temps d'arrêt du système interrompent la continuité de vos activités et ont une incidence sur vos résultats. Une étude de Gartner estime ce temps d'arrêt à une moyenne de 5 600 $ américains par minute.

Avantages de la sécurité dans le Cloud : Au-delà de la protection contre les menaces et de l'évitement des conséquences de mauvaises pratiques, la sécurité dans le Cloud offre des avantages qui en font une exigence pour les entreprises. Parmi ces avantages, on peut citer :

1. ***Sécurité centralisée :****De la même manière que l'informatique dématérialisée (cloud computing) centralise les applications et les données, la sécurité dématérialisée centralise la protection. Elle vous aide à améliorer votre visibilité, à mettre en place des contrôles et à mieux vous protéger contre les attaques. Elle améliore également la continuité de vos activités et la reprise après sinistre en ayant tout en un seul endroit.*
2. ***Réduction des coûts :***Un fournisseur de services de Cloud réputé vous proposera du matériel et des logiciels intégrés destinés à sécuriser vos applications et vos données 24/24. Vous n'aurez donc pas besoin d'investir des sommes importantes dans votre propre installation.
3. ***Administration réduite :***Le passage au Cloud introduit un modèle de responsabilité partagée en matière de sécurité. Cela peut permettre de réduire considérablement le temps et les ressources investis dans l'administration de la sécurité. Le fournisseur de services dans le Cloud assumera la responsabilité de la sécurité de son infrastructure – et de la vôtre – au niveau du stockage, de l'informatique, de la mise en réseau et de l'infrastructure physique
4. ***Fiabilité accrue :***Un fournisseur de services de Cloud de premier plan offrira du matériel et des logiciels de sécurité dématérialisée de pointe sur lesquels vous pourrez compter. Vous aurez accès à un service continu où vos utilisateurs pourront accéder en toute sécurité aux données et aux applications depuis n'importe où, sur n'importe quel appareil.

Meilleures pratiques pour la sécurité du Cloud : Lorsque vous transférez vos systèmes vers le Cloud, de nombreuses mesures de sécurité et les meilleures pratiques restent les mêmes. Toutefois, vous serez confrontés à une nouvelle série de défis que vous devrez surmonter afin de maintenir la sécurité de vos systèmes et données dans le Cloud.

La sécurité dématérialisée est un sous-domaine de la sécurité informatique et, plus largement, de la sécurité de l'information. Découvrez ces meilleures pratiques pour les déploiements basés sur le Cloud

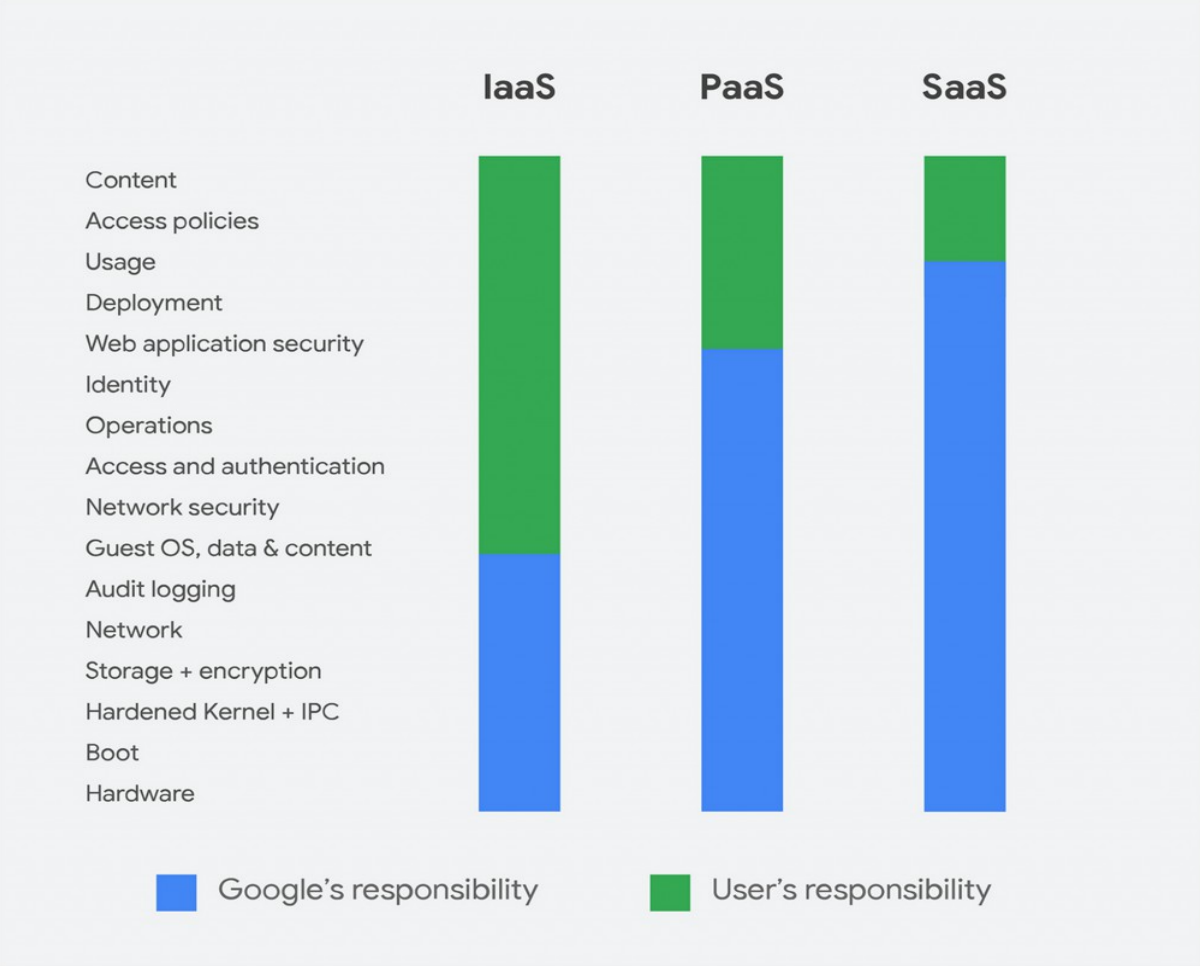
Choisir un fournisseur de confiance : Les meilleures pratiques en matière de sécurité dans le Cloud reposent sur la sélection d'un fournisseur de services de confiance. Vous souhaitez vous associer à un fournisseur de services dans le Cloud qui offre les meilleurs protocoles de sécurité intégrés et qui se conforme aux plus hauts niveaux des meilleures pratiques du secteur.Un fournisseur de services qui vous propose une place de marché de partenaires et de solutions afin d'améliorer encore la sécurité de votre déploiement.

La marque d'un fournisseur de confiance se reflète dans l'éventail des certifications et de la conformité en matière de sécurité qu'il détient. Tout bon fournisseur met ces informations à la disposition du public. Par exemple, tous les grands fournisseurs comme Amazon Web Services, Alibaba Cloud, Google Cloud (qui alimente Kinsta), et Azure offrent un accès

transparent où vous pouvez confirmer leur conformité et leurs certifications en matière de sécurité.

Au-delà de cela, de nombreux facteurs entrent en jeu dans le choix d'un fournisseur de confiance. Nous abordons ce sujet plus loin dans l'article, avec une liste de contrôle des dix principaux facteurs permettant d'évaluer la sécurité de tout fournisseur de services en ligne.

Comprendre votre modèle de responsabilité partagée : Quand vous vous associez à un fournisseur de services de Cloud et que vous transférez vos systèmes et vos données vers le Cloud, vous concluez un partenariat de responsabilité partagée pour la mise en œuvre de la sécurité.Une partie essentielle des meilleures pratiques consiste à examiner et à comprendre votre responsabilité partagée. Découvrir quelles tâches de sécurité vous incombent et quelles tâches seront désormais prises en charge par le fournisseur.Il s'agit d'une échelle mobile selon que vous optez pour le Software as a Service (SaaS), le Platform as a Service (PaaS), l'Infrastructure as a Service (IaaS) ou pour un centre de données sur site.



Les principaux fournisseurs de services en nuage comme AWS, Azure, Google Cloud Platform, et Alibaba Cloud publient ce qui est connu comme un modèle de responsabilité partagée en matière de sécurité. Garantir la transparence et la clarté. Veillez à revoir votre modèle de responsabilité partagée des fournisseurs de services de Cloud.

Examinez vos contrats et accords de niveau de service (SLA) avec les fournisseurs de services en ligne : Vous ne devriez peut-être pas envisager de revoir vos contrats et accords de niveau de service dans le cadre des meilleures pratiques de sécurité. Les contrats SLA et les contrats de services de Cloud ne sont qu'une garantie de service et de recours en cas d'incident.

Les conditions générales, les annexes et les appendices qui peuvent avoir une incidence sur votre sécurité sont beaucoup plus nombreux. Un contrat peut faire la différence entre le fait que votre fournisseur de services de Cloud soit responsable de vos données et qu'il en soit le propriétaire.

Selon le McAfee 2019 Cloud Adoption and Risk Report, 62,7 % des fournisseurs de Cloud ne précisent pas que les données des clients sont la propriété de ces derniers. Cela crée une zone d'ombre juridique où un fournisseur pourrait revendiquer la propriété de toutes vos données téléversées.Vérifiez à qui appartiennent les données et ce qu'il advient de celles-ci si vous mettez fin à vos services. Cherchez également à savoir si le fournisseur est tenu d'offrir une visibilité sur les événements et les réponses en matière de sécurité.Si vous n'êtes pas satisfait de certains éléments du contrat, essayez de négocier. Si certains ne sont pas négociables, vous devez déterminer si le fait d'accepter est un risque acceptable pour l'entreprise. Si ce n'est pas le cas, vous devrez rechercher d'autres options pour atténuer le risque par le biais du cryptage, de la surveillance ou même d'un autre fournisseur.

Formez vos utilisateurs : Vos utilisateurs constituent la première ligne de défense dans le domaine de l'informatique dématérialisée sécurisée. Leur connaissance et leur application des pratiques de sécurité peuvent faire la différence entre protéger votre système ou ouvrir une porte aux cyberattaques.

Comme meilleure pratique, assurez-vous de former tous vos utilisateurs – personnel et parties prenantes – qui accèdent à vos systèmes aux pratiques sécurisées de l'informatique dématérialiée. Sensibilisez-les à la manière de repérer les logiciels malveillants, d'identifier les e-mails de phishing et les risques de pratiques non sécurisées.

Pour les utilisateurs plus avancés – tels que les administrateurs – directement impliqués dans la mise en œuvre de la sécurité dans le Cloud, envisagez une formation et une certification spécifiques au secteur. Vous trouverez plus loin dans le guide une série de certifications et de formations recommandées en matière de sécurité dans le Cloud.

Contrôle de l'accès des utilisateurs : Mettre en œuvre un contrôle étroit des accès des utilisateurs par le biais de politiques est une autre bonne pratique de sécurité dans le Cloud. Elle vous aide à gérer les utilisateurs qui tentent d'accéder à vos services de Cloud.

Vous devez partir d'un lieu de confiance zéro, en ne donnant aux utilisateurs que l'accès aux systèmes et aux données dont ils ont besoin, rien de plus. Pour éviter la complexité lors de la mise en œuvre des politiques, créez des groupes bien définis avec des rôles attribués pour n'accorder l'accès qu'aux ressources choisies. Vous pourrez ainsi ajouter des utilisateurs directement à des groupes, plutôt que de personnaliser l'accès pour chaque utilisateur individuel.

Sécurisez vos points de terminaison (Endpoints) d'utilisateur : Un autre élément de la meilleure pratique en matière de sécurité dans les nuages est la sécurisation des points de terminaison de vos utilisateurs. La majorité des utilisateurs accèdent à vos services de Cloud par le biais de navigateurs web. Il est donc essentiel que vous introduisiez une sécurité avancée côté client pour que les navigateurs de vos utilisateurs restent à jour et protégés contre les exploitations.

Vous devriez également envisager de mettre en œuvre une solution de sécurité des points d'accès pour protéger les appareils de vos utilisateurs finaux. Vital avec l'explosion des appareils mobiles et le télétravail, où les utilisateurs accèdent de plus en plus à des services de Cloud par le biais d'appareils n'appartenant pas à l'entreprise.

Recherchez une solution qui comprend des pare-feu, des antivirus et des outils de sécurité Internet, de sécurité des appareils mobiles et de détection des intrusions.

Maintenir la visibilité de vos services en ligne :L'utilisation des services de Cloud peut être diverse et éphémère. De nombreuses organisations utilisent de multiples services de Cloud à travers un éventail de fournisseurs et de zones géographiques. Des recherches suggèrent que les ressources du Cloud ont une durée de vie moyenne de 2 heures.

Ce genre de comportement crée des angles morts dans votre environnement de Cloud. Si vous ne pouvez pas le voir, vous ne pouvez pas le sécuriser.

Veillez à mettre en place une solution de sécurité dans le Cloud qui offre une visibilité de l'ensemble de votre écosystème. Vous pourrez alors surveiller et protéger l'utilisation du Cloud dans l'ensemble de vos ressources, projets et régions disparates par le biais d'un seul portail. Cette visibilité vous aidera à mettre en œuvre des politiques de sécurité granulaires et à atténuer un large éventail de risques.

Mettre en œuvre le cryptage : Le cryptage de vos données est une bonne pratique de sécurité, quel que soir l'endroit où vous vous trouvez. En utilisant les services de Cloud, vous exposez vos données à un risque accru en les stockant sur une plateforme tierce et en les envoyant dans les deux sens entre votre réseau et le service de Cloud.Veillez à mettre en œuvre les niveaux de cryptage les plus élevés pour les données en transit et au repos. Vous devriez également envisager d'utiliser vos propres solutions de cryptage avant de téléverser des données sur le Cloud, en utilisant vos propres clés de cryptage pour garder un contrôle total.

Un fournisseur de cloud computing peut offrir des services de cryptage intégrés pour protéger vos données contre les tiers, mais cela leur permet d'accéder à vos clés de cryptage.

Kinsta exploite une approche entièrement cryptée pour mieux protéger ses solutions d'hébergement sécurisé de WordPress. Cela signifie que nous ne prenons pas en charge les connexions FTP, mais seulement les connexions cryptées SFTP et les connexions SSH.

Mettre en œuvre une politique de sécurité de mots de passe forts : Une solide politique de sécurité des mots de passe est la meilleure pratique, quel que soit le service auquel vous accédez. La mise en œuvre de la politique la plus stricte possible est un élément important pour empêcher les accès non autorisés.Au minimum, tous les mots de passe doivent comporter une lettre majuscule, une lettre minuscule, un chiffre, un symbole et un minimum de 14 caractères. Obliger les utilisateurs à mettre à jour leur mot de passe tous les 90 jours et à le paramétrer de manière à ce que le système se souvienne des 24 derniers mots de passe.Une telle politique de mots de passe empêchera les utilisateurs de créer des mots de passe simples, sur de multiples dispositifs, et permettra de se défendre contre la plupart des attaques par force brute.Comme niveau supplémentaire de protection et de bonnes pratiques en matière de sécurité, vous devez également mettre en œuvre l'authentification multifactorielle. Obligation pour l'utilisateur d'ajouter deux – ou plus – éléments de preuve pour authentifier son identité.

Utiliser un courtier en sécurité pour l'accès au Cloud (CASB) :L'utilisation d'un CASB devient rapidement un outil central pour mettre en œuvre les meilleures pratiques de sécurité dans le Cloud. Il s'agit d'un logiciel qui se situe entre vous et votre ou vos fournisseurs de services de Cloud pour étendre vos contrôles de sécurité dans le Cloud.

Un CASB vous offre un ensemble d'outils sophistiqués de sécurité dans le Cloud pour vous permettre de visualiser votre écosystème dans le Cloud, d'appliquer les politiques de sécurité des données, de mettre en œuvre l'identification et la protection des menaces et de maintenir la conformité.