Sécurisation de l'Internet des objets (IoT) avec AWS

Adoption sécurisée du cloud

Avril 2019

Avis

Ce document est uniquement fourni à titre informatif. Il présente les offres de produits et pratiques actuelles d'AWS à la date de publication de ce document, qui peuvent être modifiées sans préavis. Les clients sont chargés d'évaluer eux-mêmes et de façon indépendante les informations contenues dans ce document et toute utilisation des produits ou services d'AWS, ces derniers étant fournis « tel quel » sans garantie d'aucune sorte, qu'elle soit expresse ou implicite. Ce document ne crée aucune garantie, représentation, condition ou assurance, ni aucun engagement contractuel de la part d'AWS, de ses affiliés, fournisseurs ou concédants de licence. Les responsabilités d'AWS envers ses clients sont régies par ses accords. Ce document ne fait pas partie d'accords entre AWS et ses clients et ne les modifie pas.

Sommaire

Objectif

Ce livre blanc présente en détail les services d'Internet des objets (IoT) qui permettent aux clients de bénéficier de la sécurité dans le cloud AWS. Ce document s'adresse aux professionnels de la sécurité, aux hauts responsables qui envisagent l'adoption sécurisée de solutions IoT par l'entreprise.

Contexte

La technologie de l'IoT permet aux entreprises d'optimiser les processus, d'améliorer les offres de produits et de transformer l'expérience client de diverses façons. Bien que les chefs d'entreprise soient enthousiasmés par la façon dont leurs entreprises peuvent tirer parti de cette technologie, des préoccupations subsistent en matière de sécurité, de risque et de protection de la vie privée. Cela est dû en partie aux difficultés provoquées par des offres de sécurité disparates, incompatibles et parfois immatures qui ne permettent pas de sécuriser correctement les déploiements, ce qui entraîne un risque accru pour les données des clients ou des propriétaires d'entreprise.

Les sociétés sont désireuses de fournir des services intelligents permettant d'améliorer considérablement la qualité de vie des populations, les activités commerciales, la veille économique, la qualité des prestations des fournisseurs de services, la résilience des villes intelligentes, la durabilité environnementale et toute une série de scénarios inimaginables. Plus récemment, AWS a constaté une augmentation de l'adoption de l'IoT par les municipalités et le secteur de la santé, et d'autres secteurs devraient bientôt suivre. De nombreuses municipalités jouent un rôle de précurseur et prennent les devants en matière d'intégration des technologies modernes, comme l'IoT. On peut par exemple citer les villes suivantes :

- **Kansas City, Missouri (États-Unis) :** Kansas City a créé une plateforme de ville intelligente unifiée pour gérer les nouveaux systèmes fonctionnant le long du couloir de son tramway KC. Des capteurs vidéo, des capteurs de chaussée, des lampadaires connectés, un réseau WiFi public et la gestion du stationnement et de la circulation lui ont permis de réduire de 40 % les coûts énergétiques, soit 1,7 milliard de dollars dans le nouveau centre-ville et 3 247 nouvelles unités résidentielles.
- **Chicago, Illinois (États-Unis) :** Chicago installe des capteurs et des caméras aux intersections pour détecter le taux de pollen et la qualité de l'air pour ses citoyens.
- **Catane, Italie :** Catane a développé une application destinée à informer les navetteurs de l'emplacement de la place de stationnement libre la plus proche sur le chemin de leur destination.
- **Recife, Brésil :** Recife utilise des dispositifs de suivi placés sur tous les camions de collecte des déchets et chariots de nettoyage. La ville a ainsi pu réduire les coûts de nettoyage de 250 000 $ par mois, tout en améliorant la fiabilité des services et l'efficacité opérationnelle.
- **Newport, Pays de Galles (Royaume-Uni) :** Newport a déployé des solutions IoT pour ville intelligente afin d'améliorer la qualité de l'air, le contrôle des inondations et la gestion des déchets en seulement quelques mois.

- **Jakarta, Indonésie :** Étant une ville de 28 millions d'habitants faisant souvent face aux inondations, Jakarta exploite l'IoT pour détecter les niveaux d'eau dans les canaux et les basses terres et utilise les médias sociaux pour suivre l'opinion des citoyens. Jakarta est également en mesure de fournir des alertes rapides et d'évacuer les quartiers ciblés afin que le gouvernement et les premiers intervenants sachent quelles sont les zones qui sont le plus dans le besoin et puissent coordonner le processus d'évacuation.

Selon Machina Research, le marché mondial de l'IoT atteindra 4,3 billions de dollars d'ici 2024.[1] Selon le rapport du *Department for Business Innovation and Skills* (ministère des Entreprises, de l'Innovation et des Compétences) du Royaume-Uni, on estime que le marché mondial des solutions de ville intelligente et des services supplémentaires nécessaires pour les déployer vaudra 408 milliards de dollars d'ici 2020.[2] De plus, Forbes[3] estime que « la maintenance prédictive, l'auto-optimisation de la production et la gestion automatisée des stocks sont les trois principaux cas d'utilisation qui motiveront la croissance du marché de l'IoT jusqu'en 2020 ». Forbes affirme qu'étant donné l'impact que cela peut avoir sur le client, les entreprises souhaitent faire appel à des fournisseurs informatiques bien établis dotés d'une infrastructure fiable lors de la création ou du déploiement de solutions IoT.

Les clients souhaitent tirer parti des opportunités commerciales offertes par l'IoT. Cependant, historiquement, le caractère sécurisé de l'adoption de l'IoT n'était pas certain. Les fonctionnalités et les services sur lesquels reposaient les solutions n'étaient pas toujours sécurisés par défaut, laissant ainsi des failles de sécurité potentielles dans les fondations architecturales. De plus, sur des pratiques clés comme les communications cryptées et les mises à jour OTA, les mises à jour et la maintenance n'étaient pas automatiques. Enfin, peu de fournisseurs permettaient d'apporter des correctifs à distance aux appareils et aux passerelles après leur déploiement, ce qui les laissait vulnérables aux risques émergents en matière de sécurité.

AWS, au contraire, prend la sécurité très au sérieux en prenant en charge des millions de clients actifs originaires d'un très grand nombre de secteurs et de régions géographiques, aux exigences diverses en matière de confidentialité et de sensibilité des données. AWS investit des ressources importantes pour veiller à ce que la sécurité soit intégrée à toutes les couches de ses services et étend cette sécurité aux appareils dotés de l'IoT. La priorité d'AWS est donc de protéger la confidentialité, l'intégrité et la disponibilité des systèmes et des données des clients tout en fournissant une plateforme sûre, évolutive et sécurisée pour les solutions IoT.

Défis en matière de sécurité

Les risques et vulnérabilités existants en matière de sécurité peuvent compromettre la sécurité et la confidentialité des données des clients dans une application IoT. Associé aux données générées et au nombre croissant d'appareils, le risque de préjudice soulève des questions sur la façon de gérer les risques de sécurité posés par les appareils IoT et la communication des appareils depuis et vers le cloud.

[1] Selon https://machinaresearch.com/news/the-global-iot-market-opportunity-will-reach-usd43-trillion-by-2024.

[2] Voir https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/249423/bis-13-1217 - smart-city-market-opportunties-uk.pdf.

[3] Voir https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by - 2020 / #74c8f8c7609b.

Au niveau du risque, les préoccupations courantes des clients concernent la sécurité et le chiffrement des données pendant le transit depuis et vers le cloud, ou depuis et vers l'appareil à partir de services périphériques, ainsi que sur l'application de correctifs pour les appareils, l'authentification de ces derniers et des utilisateurs et le contrôle d'accès. La sécurisation des appareils IoT est essentielle, non seulement pour préserver l'intégrité des données, mais aussi pour les protéger contre les attaques qui peuvent avoir une incidence sur la fiabilité des appareils. Comme ces derniers peuvent envoyer de grandes quantités de données sensibles via Internet et que les utilisateurs finaux sont habilités à contrôler directement un appareil, la sécurité des « objets » doit imprégner chaque couche de la solution.

Les clients, suite aux annonces de compromission des données, surveillent la sécurité de l'IoT d'encore plus près, profitant des leçons tirées et encourageant de meilleures pratiques. La base d'une solution IoT devrait commencer et se terminer par la sécurité, ainsi que par l'utilisation de services capables d'auditer en continu les configurations IoT[4] pour s'assurer qu'elles ne s'écartent pas des bonnes pratiques en matière de sécurité. Une fois un écart détecté, des alertes doivent être déclenchées afin que les mesures correctives appropriées puissent être mises en œuvre, idéalement de manière automatique.

Pour suivre le rythme de l'entrée des appareils sur le marché ainsi que de l'arrivée des menaces en ligne, il est préférable de mettre en œuvre des services qui traitent chaque partie de l'écosystème IoT et qui se chevauchent dans leur capacité à sécuriser et protéger, contrôler et corriger, et enfin gérer les déploiements de flottes d'appareils IoT (avec ou sans connexion au cloud).

Comment les gouvernements abordent-ils la sécurité de l'IoT ?

Alors que les entreprises du secteur privé déploient activement l'IoT dans des cas d'utilisation comme les soins de santé, la construction industrielle et les biens de consommation à faible consommation, les gouvernements aux niveaux national et local commencent seulement à aborder l'adoption et la sécurité de l'IoT (voir l'annexe 2). Outre l'évaluation du futur paysage stratégique de l'IoT, AWS continue d'ajouter des services à divers cadres de conformité afin d'aider les clients à respecter leurs obligations en la matière (voir l'annexe 3).

Services et caractéristiques de sécurité d'AWS IoT

AWS propose une suite de services d'IoT pour aider les clients à sécuriser leurs appareils, leur connectivité et leurs données. Ces services permettent aux clients de tirer parti de la sécurité de bout en bout, depuis la protection des appareils jusqu'aux données en transit et au repos. Ils fournissent également des fonctionnalités de sécurité qui permettent l'application et l'exécution des stratégies de sécurité requises pour respecter leur filigrane de sécurité.

AWS IoT offre des fonctionnalités étendues et approfondies ; les clients peuvent créer des solutions IoT pour pratiquement tous les cas d'utilisation sur une large gamme d'appareils. AWS IoT s'intègre aux services d'intelligence artificielle (IA) afin que les clients puissent rendre les appareils plus intelligents, même sans connectivité Internet. Basé sur le cloud d'AWS et utilisé par des millions de clients dans 190 pays, la capacité d'AWS IoT peut être facilement ajustée à mesure que les flottes d'appareils des clients s'agrandissent et que leurs besoins opérationnels évoluent. AWS IoT offre également des fonctionnalités de sécurité complètes afin que les clients puissent créer des stratégies de sécurité

[4] Une configuration est un ensemble de contrôles techniques définis par les clients pour sécuriser les informations lorsque les appareils communiquent les uns avec les autres et avec le cloud.

préventives et répondre immédiatement aux éventuels problèmes de sécurité.

AWS IoT fournit des services cloud et des logiciels périphériques, permettant aux clients de connecter des appareils, de recueillir des données et de prendre des mesures intelligentes localement en toute sécurité, même lorsque la connectivité Internet est en panne. Les services cloud permettent aux clients d'intégrer rapidement et de connecter en toute sécurité des flottes volumineuses et diverses, de maintenir l'état et de sécuriser celles-ci et de détecter et de réagir aux événements dans les capteurs et applications IoT. Pour accélérer le développement d'applications IoT, les clients peuvent facilement connecter des appareils et des services Web à l'aide d'une interface glisser-déposer. AWS IoT peut également être utilisé pour analyser des données et créer des modèles sophistiqués d'apprentissage automatique (ML). Ces modèles peuvent être déployés dans le cloud ou sur les appareils du client afin de rendre ces derniers plus intelligents.

Bien que l'offre des services d'AWS IoT actuelle[5] est large afin de permettre des solutions IoT innovantes et complètes, ce livre blanc se concentre sur les cinq services suivants, fondamentaux pour la sécurité de l'IoT. Les descriptions des services et les caractéristiques de sécurité sont examinées plus en détail ci-dessous.

- **Amazon FreeRTOS** est un système d'exploitation open source destiné aux microcontrôleurs qui facilite la programmation, le déploiement, la sécurisation, la connexion et la gestion des petits périphériques de périmètre à faible consommation.
- **AWS IoT Greengrass** est un logiciel qui permet aux clients d'exécuter des fonctions locales de calcul, de messagerie, de mise en cache des données, de synchronisation et d'inférence ML sur des appareils connectés.
- **AWS IoT Core** est un service cloud géré qui permet aux appareils connectés d'interagir facilement et en toute sécurité avec
  des applications cloud et avec d'autres appareils.
- **AWS IoT Device Management** est un service de gestion des appareils basé sur le cloud qui facilite l'installation, l'organisation, la surveillance et la gestion à distance des appareils IoT à grande échelle en toute sécurité.
- **AWS IoT Device Defender** est un service de sécurité de l'IoT qui surveille et vérifie en permanence les configurations IoT des clients pour s'assurer qu'elles ne s'écartent pas des bonnes pratiques en matière de sécurité.

[5] Les services d'AWS IoT incluent Amazon FreeRTOS, AWS IoT Greengrass, AWS IoT Core, AWS IoT Device Management, AWS IoT Device Defender, AWS IoT Thing Graphique, AWS IoT Analytics, AWS IoT SiteWise et AWS IoT Events. Pour plus d'informations, visitez le site https://aws.amazon.com/fr/iot/.

Amazon FreeRTOS — Logiciel de périphérique

Présentation du service : Amazon FreeRTOS (a : FreeRTOS) est un système d'exploitation open source destiné aux microcontrôleurs[6] qui facilite la programmation, le déploiement, la sécurisation, la connexion et la gestion des petits périphériques de périmètre à faible consommation. Amazon FreeRTOS est basé sur le noyau FreeRTOS, un système d'exploitation open source populaire pour les microcontrôleurs, et le renforce avec des bibliothèques logicielles qui facilitent la connexion sécurisée directe entre les petits appareils à faible consommation des clients et les services du Cloud AWS comme AWS IoT Core, ou des périphériques de périmètre plus puissants exécutant AWS IoT Greengrass.

Caractéristiques de sécurité : Amazon FreeRTOS est livré avec des bibliothèques afin de sécuriser les données et les connexions des appareils, y compris la prise en charge du chiffrement des données et de la gestion des clés. Amazon FreeRTOS inclut la prise en charge du protocole Transport Layer Security (TLS v1.2) pour aider les appareils à se connecter en toute sécurité au cloud. Amazon FreeRTOS dispose également d'une fonction de signature de code permettant de garantir que le code de l'appareil du client n'est pas compromis pendant le déploiement. Il dispose enfin de fonctionnalités permettant aux mises à jour OTA de mettre à jour des appareils à distance avec des améliorations de fonctionnalités ou des correctifs de sécurité.

AWS IoT Greengrass — Logiciel pour l'edge computing

Présentation du service : AWS IoT Greengrass est un logiciel qui permet aux clients d'exécuter des fonctions locales de calcul, de messagerie, de mise en cache des données, de synchronisation et d'inférence ML pour les appareils connectés,[7] ce qui permet aux appareils connectés de fonctionner même avec une connectivité intermittente au cloud. Une fois l'appareil reconnecté, AWS IoT Greengrass synchronise les données de l'appareil avec AWS IoT Core, fournissant ainsi des fonctionnalités constantes indépendamment de la connectivité. AWS IoT Greengrass étend de manière transparente AWS aux appareils afin qu'ils puissent agir localement sur les données qu'ils génèrent, tout en utilisant le cloud pour la gestion, l'analyse, et le stockage durable.

Caractéristiques de sécurité : AWS IoT Greengrass authentifie et crypte les données des appareils pour les communications locales et cloud. Les données ne sont jamais échangées entre les appareils et le cloud sans que l'identité ne soit prouvée. Le service utilise une gestion de la sécurité et des accès similaire à ce que les clients connaissent dans AWS IoT Core, avec l'authentification et l'autorisation mutuelles des appareils, ainsi qu'une connectivité sécurisée au cloud.

[6] Un microcontrôleur est une puce unique contenant un processeur simple qui peut être trouvé dans de nombreux appareils, y compris les appareils électroménagers, les moniteurs d'activité physique, les capteurs d'automatisation industrielle et les voitures. Beaucoup de ces petits appareils pourraient bénéficier d'une connexion locale à d'autres appareils ou d'une connexion au cloud. Par exemple, les compteurs d'électricité intelligents doivent se connecter au cloud pour générer des rapports d'utilisation, et les systèmes de sécurité des bâtiments doivent communiquer localement afin qu'une porte se déverrouille lorsque quelqu'un passe son badge.

[7] Pour commencer à utiliser AWS IoT Greengrass, les clients auront besoin d'un appareil capable d'exécuter le noyau d'AWS IoT Greengrass. Vous trouverez une liste complète des appareils qualifiés et des dépendances techniques ici. Cliquez ici pour obtenir un guide pratique de mise en route. Les clients peuvent trouver la référence détaillée du développeur ici.

Plus précisément, AWS IoT Greengrass utilise des certificats X.509[8], des abonnements gérés, des stratégies AWS IoT et des politiques de gestion des identités et des accès (GIA) AWS pour s'assurer que les applications AWS IoT Greengrass sont sécurisées. Les appareils AWS IoT nécessitent un objet AWS IoT, un certificat de périphérique et une stratégie AWS IoT pour se connecter au service AWS IoT Greengrass. Cela permet aux appareils principaux d'AWS IoT Greengrass de se connecter en toute sécurité au service cloud d'AWS IoT. Cela permet également au service cloud AWS IoT Greengrass de déployer des informations de configuration, des fonctions AWS Lambda et des abonnements gérés sur des appareils principaux AWS IoT Greengrass. En outre, AWS IoT Greengrass fournit une racine de confiance matérielle de stockage de clés privées pour les périphériques de périmètre.

D'autres fonctionnalités de sécurité importantes d'AWS IoT Greengrass sont la surveillance et la journalisation. Les logiciels de base du service peuvent par exemple écrire des journaux sur Amazon CloudWatch[9] (fonctionne également pour AWS IoT Core) et sur le système de fichiers local des appareils principaux des clients. La journalisation est configurée au niveau du groupe et sur AWS IoT Greengrass, toutes les entrées de journal incluent un horodatage, un niveau de journalisation et des informations sur l'événement. AWS IoT Greengrass est intégré à AWS CloudTrail[10], un service fournissant un enregistrement des actions effectuées par un utilisateur, un rôle ou un service AWS dans AWS IoT Greengrass. S'il est activé par le client, il capture tous les appels d'interface de programmation d'applications (API) pour AWS IoT Greengrass en tant qu'événements. Cela inclut les appels depuis la console AWS IoT Greengrass et les appels de code vers les opérations de l'API AWS IoT Greengrass. Les clients peuvent par exemple créer un journal de suivi et les appels peuvent permettre la livraison continue d'événements AWS CloudTrail vers un compartiment Amazon Simple Storage Service (Amazon S3), y compris des événements pour AWS IoT Greengrass. Si les clients ne souhaitent pas créer un journal de suivi, ils peuvent afficher les événements les plus récents dans la console AWS CloudTrail dans l'historique des événements (si activée). Ces informations peuvent être utilisées pour effectuer un certain nombre de tâches, comme déterminer quand une demande a été faite à AWS IoT Greengrass et l'adresse IP à partir de laquelle la demande a été faite.

Des options sont disponibles en matière de bonnes pratiques pour sécuriser les données des clients sur l'appareil et doivent être utilisées chaque fois que possible. Pour AWS IoT Greengrass, tous les appareils IoT doivent activer le chiffrement complet du disque et suivre les bonnes pratiques de gestion des clés. Les clients peuvent utiliser le cryptage complet du disque, en utilisant des clés AES 256 bits basées sur les algorithmes validés de la norme FIPS 140-2 du NIST[11] et suivre les bonnes pratiques de gestion des clés. Pour les appareils à faible consommation tels que ceux qui utilisent Amazon FreeRTOS, les clients peuvent suivre les recommandations de chiffrement léger du rapport NIST 8114[12].

---

[8] Les certificats X.509 sont des certificats numériques qui utilisent la norme d'infrastructure à clé publique X.509 pour associer une clé publique à une identité contenue dans un certificat. Les certificats X.509 sont émis par une entité de confiance appelée autorité de certification (CA). L'autorité de certification gère un ou plusieurs certificats spéciaux appelés certificats CA qu'elle utilise pour émettre des certificats X.509. Seule l'autorité de certification a accès aux certificats CA. Voir https://docs.aws.amazon.com/fr_fr/iot/latest/developerguide/x509-certs.html pour plus d'informations.

[9] Voir https://aws.amazon.com/fr/cloudwatch/.

[10] Voir https://aws.amazon.com/fr/cloudtrail/.

[11] Algorithmes cryptographiques approuvés FIPS 140-2 du NIST : https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf.

[12] NIST 8114 : chiffrement léger : https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

Les sections ci-dessus portaient sur les microcontrôleurs et les cas d'utilisation en périphérie. Ci-dessous, le document se concentrera sur les services IoT fonctionnant dans le cloud.

AWS IoT Core : passerelle IoT basée sur le cloud

Présentation du service : AWS IoT Core est un service cloud géré qui permet aux appareils connectés d'interagir facilement et en toute sécurité avec les applications cloud et avec d'autres appareils. AWS IoT Core offre une communication et un traitement de données sécurisés pour différents types d'appareils et d'emplacements connectés afin que les clients puissent facilement créer des applications IoT. Parmi les exemples d'utilisation des clients, citons les solutions industrielles et les solutions domestiques connectées pouvant prendre en charge des milliards d'appareils et des billions de messages qui peuvent être traités et acheminés vers des terminaux AWS et d'autres appareils de manière fiable et sécurisée.

Caractéristiques de sécurité : AWS IoT Core offre aux clients un certain nombre de solutions qui permettent d'assurer et de maintenir la sécurité. Les mécanismes de sécurité du cloud AWS protègent les données lors de leur déplacement entre AWS IoT et d'autres appareils ou services AWS. Les appareils peuvent se connecter à l'aide de diverses options d'identité (certificats X.509, utilisateurs et groupes IAM,
Identités Amazon Cognito ou jetons d'authentification personnalisés) via une connexion sécurisée. Tandis que les clients effectuent les validations côté client (validation de la chaîne de confiance, vérification du nom d'hôte, stockage sécurisé et distribution de leurs clés privées), AWS IoT Core fournit des canaux de transport sécurisés à l'aide du protocole TLS. Le moteur de règles d'AWS IoT transmet également les données de l'appareil à d'autres appareils et services AWS conformément aux règles définies par le client. Les systèmes de gestion des accès AWS sont utilisés pour transférer les données vers leur destination finale en toute sécurité. Une autre fonctionnalité d'autorisation d'AWS IoT mérite d'être notée : les variables de stratégie d'AWS IoT, qui permet d'éviter la fourniture d'informations d'identification privilégiées sur un appareil. Ces fonctionnalités, utilisées conjointement avec les bonnes pratiques générales en matière de cybersécurité, permettent de protéger les données des clients.

AWS IoT Device Management : service de gestion des appareils IoT basé sur le cloud

Présentation du service : AWS IoT Device Management aide les clients à intégrer, organiser, surveiller et gérer à distance les appareils IoT à grande échelle. AWS IoT Device Management s'intègre à AWS IoT Core afin de connecter facilement les appareils au cloud et à d'autres appareils pour que les clients puissent gérer à distance leurs flottes d'appareils. AWS IoT Device Management aide les clients à intégrer de nouveaux appareils en utilisant AWS IoT au sein d'AWS Management Console ou d'une API pour télécharger des modèles qu'ils remplissent avec des informations telles que le fabricant de l'appareil et le numéro de série, les certificats d'identité X.509 ou les stratégies de sécurité. Les clients peuvent ensuite configurer l'ensemble de la flotte d'appareils avec ces informations en quelques clics dans AWS IoT au sein d'AWS Management Console.

Caractéristiques de sécurité : Avec AWS IoT Device Management, les clients peuvent regrouper leur flotte d'appareils selon une structure hiérarchique basée sur la fonction, les exigences de sécurité ou des catégories similaires. Ils peuvent créer des groupes constitués d'un seul appareil dans une pièce, de plusieurs appareils au même étage ou de tous les appareils fonctionnant dans un bâtiment. Ces groupes peuvent ensuite être utilisés pour gérer des stratégies d'accès, afficher des mesures opérationnelles ou effectuer des actions sur l'ensemble du groupe. En outre, une fonctionnalité appelée « Objets dynamiques » peut automatiquement ajouter des appareils répondant aux critères définis par le client et supprimer ceux qui ne correspondent plus aux exigences. Cela rationalise le processus en toute sécurité tout en préservant l'intégrité opérationnelle. Cette fonction facilite également la recherche d'enregistrements d'appareils selon n'importe quelle combinaison d'attributs et permet aux clients d'effectuer des mises à jour en bloc.

Grâce à AWS IoT Device Management, les clients peuvent également envoyer des logiciels et des micrologiciels sur des appareils sur le terrain pour corriger les vulnérabilités de sécurité et améliorer les fonctionnalités des appareils ; exécuter des mises à jour en bloc ; contrôler la vitesse de déploiement ; définir des seuils d'échec et définir des tâches continues pour la mise à jour automatique du logiciel des périphériques afin que ces derniers exécutent toujours la dernière version du logiciel. Les clients peuvent déclencher des actions à distance, comme des redémarrages de l'appareil ou des réinitialisations d'usine, pour résoudre les problèmes logiciels de l'appareil ou restaurer ses paramètres d'origine. Les clients peuvent également signer les fichiers envoyés sur leurs appareils de façon numérique, ce qui permet de s'assurer qu'ils ne sont pas compromis.

La possibilité d'envoyer des mises à jour logicielles ne se limite pas aux services cloud. En réalité, les tâches de mise à jour OTA dans Amazon FreeRTOS permettent aux clients d'utiliser AWS IoT Device Management pour planifier des mises à jour logicielles. De la même manière, les clients peuvent créer une tâche de mise à jour du noyau d'AWS IoT Greengrass pour un ou plusieurs appareils principaux AWS IoT Greengrass grâce à AWS IoT Device Management afin de déployer des mises à jour de sécurité, des correctifs de bogues et des nouvelles fonctionnalités AWS IoT Greengrass pour les appareils connectés.

AWS IoT Device Defender : service de sécurité des appareils IoT basé sur le cloud

Présentation du service : AWS IoT Device Defender est un service entièrement géré qui aide les clients à vérifier les fonctionnalités de sécurité établies pour leur flotte d'appareils IoT. Le service vérifie en permanence les configurations IoT pour s'assurer qu'elles ne s'écartent pas des bonnes pratiques de sécurité en matière de maintien et d'application des configurations IoT, telles que la garantie de l'identité, l'authentification et l'autorisation et le chiffrement des données des appareils. Le service peut envoyer une alerte s'il existe des lacunes dans la configuration IoT d'un client pouvant créer un risque pour la sécurité, telles que le partage sur plusieurs appareils de certificats d'identité ou la tentative de connexion à AWS IoT Core d'un appareil au certificat d'identité révoqué.

Caractéristiques de sécurité : Outre les fonctions de surveillance et d'audit du service, les clients peuvent définir des alertes correctives afin de remédier aux écarts constatés dans les appareils. Par exemple, les pics de trafic sortant peuvent indiquer qu'un appareil participe à une attaque par déni de service distribué (DDoS). AWS IoT Greengrass et Amazon FreeRTOS s'intègrent également automatiquement à AWS IoT Device Defender pour fournir des mesures de sécurité d'appareils à des fins d'évaluation.

AWS IoT Device Defender peut envoyer des alertes à AWS IoT, Amazon CloudWatch et Amazon Simple Notification Service (Amazon SNS), comprenant des alertes qui sont transmises sur les mesures d'Amazon CloudWatch. Si un client décide de traiter une alerte, AWS IoT Device Management peut être utilisé pour prendre des mesures d'atténuation telles que l'envoi de correctifs de sécurité.

AWS IoT Device Defender vérifie les configurations IoT associées aux appareils des clients selon un ensemble de bonnes pratiques définies en matière de sécurité IoT afin que les clients puissent voir où les lacunes de sécurité existent et exécuter des audits de façon continue ou ad hoc. Des pratiques de sécurité existent également au sein d'AWS IoT Device Defender et peuvent être sélectionnées et exécutées dans le cadre de l'audit. Ce service s'intègre aussi à d'autres services AWS, tels qu'Amazon CloudWatch et

Amazon SNS, afin d'envoyer des alertes de sécurité à AWS IoT lorsqu'un audit échoue ou lorsque des anomalies de comportement sont détectées pour que les clients puissent étudier et déterminer la cause première. Par exemple, AWS IoT Device Defender peut alerter les clients lorsque les identités d'appareils accèdent aux API sensibles. AWS IoT Device Defender peut également recommander des actions réduisant l'impact des problèmes de sécurité tels que la révocation des autorisations, le redémarrage d'un appareil, la réinitialisation des paramètres d'usine ou l'envoi de correctifs de sécurité sur les appareils connectés des clients.

Les clients peuvent également être préoccupés par les mauvais acteurs : les erreurs humaines ou systémiques et les utilisateurs autorisés ayant des intentions malveillantes peuvent en effet introduire des configurations ayant un impact négatif sur la sécurité. AWS IoT Core fournit les modules de sécurité permettant aux clients de connecter en toute sécurité des appareils au cloud et à d'autres appareils. Ces modules permettent d'appliquer des contrôles de sécurité tels que l'authentification, l'autorisation, la journalisation des audits et le chiffrement de bout en bout. Ensuite, AWS IoT Device Defender intervient et aide à auditer en permanence les configurations de sécurité afin de garantir leur conformité aux bonnes pratiques de sécurité et aux politiques de sécurité propres aux entreprises des clients.

Tirer parti de la sécurité prouvable pour améliorer l'IoT : notre avantage concurrentiel

De nouveaux services et de nouvelles technologies de sécurité sont en cours d'élaboration chez AWS pour aider les entreprises à sécuriser leur IoT et leurs périphériques de périmètre. AWS a notamment lancé récemment des vérifications au sein d'AWS IoT Device Defender, optimisées par une technologie d'IA appelée raisonnement automatisé, qui exploite des preuves mathématiques pour vérifier que le logiciel est écrit correctement et déterminer s'il existe un accès non intentionnel aux appareils. AWS IoT Device Defender illustre une des manières dont les clients peuvent utiliser le raisonnement automatisé de façon directe afin de sécuriser leurs propres appareils. En interne, AWS a utilisé un raisonnement automatisé pour vérifier l'intégrité de la mémoire du code s'exécutant sur Amazon FreeRTOS et se protéger contre les logiciels malveillants. L'investissement dans le raisonnement automatisé afin de fournir une assurance évolutive que le logiciel est sécurisé, appelée « sécurité de contrôle », permet aux clients d'exploiter des charges de travail sensibles sur AWS.

AWS Zelkova[13][13] utilise un raisonnement automatisé pour prouver que les contrôles d'accès aux données des clients fonctionnent comme prévu. Les vérifications des contrôles d'accès d'AWS IoT Device Defender sont optimisées par Zelkova, ce qui permet aux clients de s'assurer que leurs données sont correctement protégées. Une stratégie AWS IoT est trop permissive si elle autorise l'accès à des ressources en dehors de la configuration de sécurité prévue par un client. Les commandes optimisées par Zelkova intégrées dans AWS IoT Device Defender vérifient que les stratégies n'autorisent pas les actions limitées par la sécurité du client et que les ressources prévues disposent des autorisations nécessaires pour effectuer certaines actions.

D'autres outils automatisés basés sur le raisonnement ont permis de sécuriser les bases de l'infrastructure AWS IoT. Un outil open source appelé CBMC a été utilisé pour prouver l'exactitude d'Amazon FreeRTOS, donnant ainsi davantage confiance aux clients pour leur exécution de charges de travail sur des appareils Amazon IoT. Cela garantit qu'aucun attaquant ne peut exploiter ou obtenir un accès non autorisé à Amazon FreeRTOS. Les mécanismes de contrôle du raisonnement automatisé d'Amazon FreeRTOS ont été continuellement intégrés pour vérifier les mises à jour apportées au système d'exploitation. Ainsi, chaque fois qu'un changement de code est effectué, des mesures sont mises en place pour permettre aux développeurs AWS de vérifier automatiquement la sûreté de la mémoire du logiciel Amazon FreeRTOS.

Le raisonnement automatisé continue d'être mis en œuvre pour un grand nombre de services et de fonctionnalités AWS, offrant des niveaux d'assurance de sécurité accrus pour les composants critiques du cloud AWS. AWS continue de déployer un raisonnement automatisé pour développer des outils pour les clients ainsi que des technologies de vérification de l'infrastructure interne pour la pile AWS IoT.

[13] Pour en savoir plus sur Zelkova, consultez https://aws.amazon.com/blogs/security/protect-sensitive-data-in-the-cloud-with-automated - raisoning-zelkova.

Quelles sont les bonnes pratiques clés en matière de sécurité de l'IoT ?

Malgré le nombre de bonnes pratiques disponibles, il n'existe pas d'approche unique permettant d'atténuer les risques liés aux solutions IoT. Selon l'appareil, le système, le service et l'environnement dans lequel les appareils sont déployés, les clients peuvent prendre en compte différentes menaces, vulnérabilités et tolérances au risque. Voici les pratiques recommandées lors de l'intégration de la sécurité de bout en bout aux données, appareils et services cloud :

1. **Intégrer la sécurité à la phase de conception**
   La base d'une solution IoT commence et se termine par la sécurité. Comme les appareils peuvent envoyer de grandes quantités de données sensibles et qu'il est possible que les utilisateurs finaux d'applications IoT puissent contrôler directement un appareil, la sécurité des « objets » doit être une exigence de conception omniprésente. La sécurité n'est pas une formule statique ; les applications IoT doivent pouvoir modéliser, surveiller et itérer en permanence les bonnes pratiques en la matière.
   Le cycle de vie d'un appareil physique et le matériel limité utilisé pour les capteurs, les microcontrôleurs, les actionneurs et les bibliothèques intégrés représentent un défi pour la sécurité de l'IoT. Ces facteurs limités peuvent restreindre les fonctionnalités de sécurité que chaque appareil peut exécuter. Avec ces dynamiques supplémentaires, les solutions IoT doivent constamment adapter leur architecture, leur microprogramme et leur logiciel pour rester en avance sur l'évolution du paysage de la sécurité. Bien que les facteurs limités des appareils puissent présenter des risques accrus, des obstacles et des compromis potentiels entre la sécurité et les coûts, l'objectif principal de toute entreprise doit être la création d'une solution IoT sécurisée.

2. **S'appuyer sur des cadres reconnus en matière de sécurité informatique et de cybersécurité**
   AWS prend en charge une approche ouverte et basée sur des normes pour promouvoir l'adoption sécurisée de l'IoT. Lorsque l'on considère les milliards d'appareils et de points de connexion nécessaires pour prendre en charge un écosystème IoT robuste à des fins d'utilisation par des consommateurs, l'industrie et le secteur public, l'interopérabilité est essentielle. Les services AWS IoT respectent ainsi les protocoles standard et les bonnes pratiques du secteur. AWS IoT Core prend par ailleurs en charge d'autres normes industrielles et protocoles personnalisés du secteur, ce qui permet aux appareils de communiquer entre eux, même s'ils utilisent des protocoles différents. AWS est un ardent défenseur de l'interopérabilité afin que les développeurs puissent s'appuyer sur les plateformes existantes pour répondre à l'évolution des besoins des clients. AWS prend également en charge un écosystème de partenaires florissant afin d'élargir le menu des choix et étendre les limites de ce qui est possible pour les clients.

L'application des bonnes pratiques reconnues mondialement présente un certain nombre d'avantages pour toutes les parties prenantes d'IoT, notamment :

- Répétabilité et réutilisation, au lieu de reprendre à zéro
- Cohérence et consensus pour promouvoir la compatibilité des technologies et l'interopérabilité au-delà des frontières géographiques
- Optimisation de l'efficacité pour accélérer la modernisation et la transformation des TI

3. **Mettre l'accent sur l'impact afin de hiérarchiser les mesures de sécurité**

   Les attaques ou les anomalies ne sont pas identiques et peuvent ne pas avoir le même impact sur les personnes, les opérations commerciales et les données. La compréhension des écosystèmes IoT des clients et de l'endroit où les appareils fonctionneront au sein de cet écosystème permet de prendre des décisions éclairées sur l'endroit où les risques les plus élevés : au sein de l'appareil, dans le cadre du réseau, ou des composants physiques ou de la sécurité. Il est essentiel de se concentrer sur l'évaluation de l'impact des risques et sur les conséquences pour déterminer les points vers lesquels les efforts de sécurité devraient être dirigés, et qui est responsable de ces efforts dans l'écosystème IoT.

Conclusion

Outre une croissance exponentielle des appareils connectés, chaque « objet » dans IoT communique des paquets de données qui nécessitent une connectivité, un stockage et une sécurité fiables. Avec l'IoT, une entreprise est confrontée à la gestion, à la surveillance et à la sécurisation d'immenses volumes de données et de connexions depuis des appareils dispersés. Mais ce défi ne doit pas nécessairement représenter un obstacle dans un environnement basé sur le cloud. En plus de la mise à l'échelle et du développement d'une solution dans un endroit unique, le cloud computing permet aux solutions IoT d'évoluer à l'échelle mondiale et dans différents emplacements physiques tout en réduisant la latence des communications et en permettant une meilleure réactivité depuis des appareils sur le terrain. AWS offre une suite de services IoT possédant une sécurité de bout en bout, y compris des services permettant d'exploiter et de sécuriser les points de terminaison, les passerelles, les plateformes, et les applications, ainsi que le trafic traversant ces couches. Cette intégration simplifie l'utilisation et la gestion sécurisées des appareils et des données qui interagissent en permanence les uns avec les autres, ce qui permet aux entreprises de bénéficier de l'innovation et de l'efficacité que peut offrir IoT tout en maintenant la sécurité comme priorité.

Annexe 1 — Intégration des services AWS IoT

AWS IoT s'intègre directement aux services AWS suivants :

- **Amazon Simple Storage Service (Amazon S3),** qui fournit un stockage évolutif dans le cloud AWS. Pour plus d'informations, consultez Amazon S3.
- **Amazon DynamoDB,** qui fournit des bases de données NoSQL gérées. Pour plus d'informations, consultez Amazon DynamoDB.
- **Amazon Kinesis,** qui permet un traitement en temps réel des données de streaming à grande échelle. Pour plus d'informations, consultez Amazon Kinesis.
- **AWS Lambda,** qui exécute le code des clients sur des serveurs virtuels à partir d'Amazon Elastic Compute Cloud (Amazon EC2) en réponse à des événements. Pour plus d'informations, consultez AWS Lambda.
- **Amazon Simple Notification Service (Amazon SNS),** qui envoie ou reçoit des notifications. Pour plus d'informations, consultez Amazon SNS.
- **Amazon Simple Queue Service (Amazon SQS),** qui stocke les données dans une file d'attente afin que les applications puissent les récupérer.
  Pour plus d'informations, consultez Amazon SQS.

Annexe 2 — Les gouvernements s'attaquant à l'IoT

États-Unis

Le National Institute of Standards and Technology (NIST) — ministère du Commerce

Le ministère du Commerce des États-Unis est le fer de lance de multiples efforts visant à aborder la question de la sécurité de l'IoT. Le National Institute of Standards and Technology (NIST) a publié un livre blanc[14] qui met en lumière des sujets dont les clients et les organismes gouvernementaux tiennent compte lorsqu'ils évaluent la sécurité des données et des appareils. Dans le livre blanc, les lecteurs sont invités à évaluer ces préoccupations et reçoivent des recommandations sur la façon d'atténuer les problèmes. Le NIST a également publié le NIST Internal Report (NISTIR) 8228,[15] qui identifie les risques susceptibles d'avoir un impact négatif sur l'adoption de l'IoT. Le document contient par ailleurs des recommandations visant à atténuer ou à réduire les effets de ces préoccupations. Le NIST organise en outre des partenariats publics et privés, sollicite des commentaires et organise des ateliers sur les villes intelligentes et la normalisation internationale de l'IoT, entre autres initiatives[16]. Bien qu'à ses balbutiements, les premiers indicateurs indiquent que les risques potentiels de cybersécurité et de protection de la vie privée représentent des obstacles sérieux aux profits que les gouvernements et les consommateurs pourraient tirer de l'IoT.

Ministère de la Défense

La communauté de la défense offre un autre exemple au sein du gouvernement. En 2016, le directeur des systèmes d'information du ministère de la Défense (DoD) des États-Unis a formulé des recommandations quant aux politiques à mettre en œuvre afin de remédier aux vulnérabilités et aux risques liés à l'IoT[17]. Selon ces recommandations, le DoD dote déjà les installations, les véhicules et les dispositifs médicaux du DoD de millions de dispositifs et de capteurs IoT et envisage de les intégrer dans les armes et les systèmes de renseignement. La complexité de la sécurisation de l'IoT provient de la puissance de traitement limitée des appareils à exécuter des pare-feu et des logiciels anti-programmes malveillants, ainsi que du grand nombre d'appareils, qui aggravent l'exposition à la vulnérabilité à un niveau différent de celui des appareils mobiles traditionnels.

L'approche et l'action politique recommandées par le DoD pour faire face aux risques de sécurité de l'IoT sont les suivantes : 1) une analyse des risques liés à la sécurité et à la vie privée soutenant chaque mise en œuvre de l'IoT et les flux de données associés, 2) le chiffrement à chaque point, où les coûts sont proportionnels au risque et à la valeur, et 3) la surveillance des réseaux IoT pour identifier le trafic anormal et les menaces émergentes.

[14] Jeffrey Voas (NIST), Richard Kuhn (NIST), Phillip Laplante (Penn State University) et Sophia Applebaum (MITRE), « Internet of Things (IoT) Trust Concerns » (16 octobre 2018, https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft.)

[15] NISTIR 8228, « Consideations for Managing IoT Cybersecurity and Privacy Risks Out for Public Comments » (26 septembre 2018, https://www.nist.gov/news-events/news/2018/09/draft-nistir-8228-considerations-managing-iot-cybersecurity-and-privacy.)

[16] Voir https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot.

[17] Voir https://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20 Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440.

Commission fédérale du commerce (FTC)

La FTC a joué un rôle important dans les conversations sur la sécurité de l'IoT, en poursuivant en justice des fabricants d'appareils ayant donné une image déformée de leurs engagements en matière de sécurité ou ayant démontré une négligence dans ce domaine. La FTC s'est fixé comme objectif une « sécurité raisonnable des données ».

La FTC a relevé les lacunes répétées suivantes en matière de sécurité chez les fabricants d'appareils :

- Sécurité non intégrée aux appareils
- Développeurs ne formant pas leurs employés sur les bonnes pratiques de sécurité
- Non-garantie de la sécurité et de la conformité en aval (via des contrats)
- Absence de défense dans les stratégies de fond
- Absence de contrôles d'accès raisonnables (les clients peuvent contourner ou deviner les mots de passe par défaut)
- Absence de programme de sécurité des données

État de Californie

La Californie est l'un des premiers États américains à adopter une législation sur l'IoT. Les projets de loi actuels traitent de questions telles que la sécurité de la conception des appareils et la protection des données, mais n'ont pas d'exigences spécifiques concernant les fabricants d'IoT. À la place, les législateurs se sont concentrés sur la sécurité au stade de la conception, en écrivant que la protection des données doit être « adaptée à la nature et à la fonction de l'appareil » et « adaptée aux informations qu'il peut recueillir, contenir ou transmettre ».

Royaume-Uni

Le *Department for Digital, Culture, Media and Sport* (ministère du Numérique, de la Culture, des Médias et du Sport ou « DCMS ») du Royaume-Uni a publié la version finale de son Code de pratique pour la sécurité de l'IoT à destination du grand public (Code of Practice for Consumer IoT Security) en octobre 2018[18]. Ce code de pratique a été rédigé conjointement avec le Centre national de cybersécurité et comprenait des commentaires de membres d'associations de consommateurs, de l'industrie et du milieu universitaire. Le document fournit 13 lignes directrices sur la façon de parvenir à une approche « sécurisée de par conception » pour toutes les entreprises impliquées dans le développement, la fabrication et la vente au détail de produits IoT à destination du grand public.

[18] Voir https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security.

Le Code de bonnes pratiques met l'accent sur trois pratiques exemplaires afin de permettre aux utilisateurs d'obtenir les avantages les plus importants et immédiats en matière de sécurité, et exhorte les parties prenantes IoT à les hiérarchiser : 1) aucun mot de passe par défaut : de nombreux utilisateurs ne modifient pas le mot de passe par défaut, ce qui a été la source de nombreux problèmes de sécurité de l'IoT ; 2) mise en place d'une politique de divulgation des vulnérabilités : les développeurs d'appareils, de services et d'applications IoT devraient disposer d'une politique de divulgation des vulnérabilités et d'un point de contact public pour permettre le signalement (et la correction) des vulnérabilités en temps opportun ; 3) maintien à jour du logiciel : les mises à jour logicielles doivent être rapides, faciles à mettre en œuvre et ne pas perturber le fonctionnement de l'appareil.

Compte tenu des préoccupations et des approches exposées par les États-Unis et le Royaume-Uni, la sécurité de l'IoT continuera d'être une priorité pour les gouvernements. Des efforts sont également entrepris par les organismes nationaux et internationaux de normalisation pour élaborer des normes, des lignes directrices et des bonnes pratiques en matière de sécurisation de l'IoT[19] y compris l'architecture de référence pour l'IoT de l'Organisation internationale de normalisation (ISO) et le groupe d'étude sur l'IoT et les villes intelligentes de l'Union internationale des télécommunications (UIT).[20]

Dans le contexte de l'IoT, les clients devraient avoir la flexibilité nécessaire pour utiliser des pratiques existantes et éprouvées déjà utilisées dans ce qui est considéré comme une « cybersécurité des réseaux plus traditionnelle ». Les clients peuvent par exemple utiliser les contrôles de cybersécurité mis en correspondance avec le NIST Cybersecurity Framework (CSF).[21] Lorsqu'ils essaient d'identifier les vulnérabilités, de détecter les irrégularités, de réagir à des incidents potentiels et de récupérer après des dommages ou des perturbations causés à des appareils IoT. Cet ensemble fondamental de disciplines de la cybersécurité est reconnu à l'échelle mondiale et a reçu l'appui des gouvernements et des industries comme étant une référence recommandée à toute organisation, quel que soit son secteur ou sa taille. L'avantage d'utiliser le CSF du NIST ne réside pas seulement dans sa réputation, mais aussi dans la flexibilité qu'il permet dans l'application de la cybersécurité tout en gardant à l'esprit son effet sur les dimensions physique, cybernétique et humaine. Outre l'aspect humain, le cadre s'applique aux entreprises qui s'appuient sur la technologie, que l'accent soit mis principalement sur les technologies de l'information, les systèmes de contrôle industriel, les systèmes cyberphysiques ou l'IoT.

[19] Pour obtenir un recueil des normes et initiatives actuelles en matière de sécurité de l'IoT, consultez le catalogue de la NTIA (National Telecommunications and Information Administration) du ministère du Commerce américain : https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_17.pdf.

[20] Voir https://www.itu.int/fr/ITU-T/about/groups/Pages/sg20.aspx.

[21] Pour plus d'informations sur la manière de s'aligner sur le CSF du NIST à l'aide des services d'AWS, reportez-vous à ce livre blanc et à ce manuel client : https://do.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf.

Annexe 3 — Services AWS IoT et conformité

En tant que fournisseur mondial de services cloud Hyperscale, AWS adopte une approche rigoureuse basée sur les risques en ce qui concerne la sécurité de ses services IoT et la protection des données des clients. AWS applique les processus de sécurité internes sur tous ses services cloud afin d'évaluer l'efficacité des contrôles techniques, opérationnels et de gestion nécessaires à la protection contre les menaces actuelles et émergentes ayant une incidence sur la sécurité et la résilience. Ce processus obligatoire d'assurance de la sécurité se traduit non seulement par l'attestation de divers cadres de conformité, mais aussi par l'engagement d'AWS d'intégrer la sécurité à toutes les phases du développement et des processus opérationnels du cycle de vie de ses services. AWS propose des services de cloud commercial hyperscale qui ont été accrédités selon des normes internationales reconnues, telles que la norme 27001 de l'Organisation internationale de normalisation (ISO)[22], la norme PCI (Payment Card Industry Data Security Standard)[23], et la norme SOC (service Organization Control Reports) [24][24], entre autres accréditations internationales, nationales et sectorielles. AWS répond également aux exigences de sécurité rigoureuses en matière de prise en charge des environnements classifiés de certaines agences de renseignement. Globalement, les clients utilisant les services cloud d'AWS, quel que soit leur secteur et quelle que soit leur taille obtiennent des avantages en matière de sécurité par procuration, car AWS s'applique à fournir la plus haute qualité sur tous ses services.

AWS est sensible au fait que les clients peuvent avoir des exigences de conformité spécifiques qui doivent être démontrées et respectées. En gardant cela à l'esprit, AWS ajoute continuellement des services s'alignant sur les programmes de conformité en fonction de la demande des clients. Les services IoT visés sont répertoriés par programme de conformité sur le site Web d'AWS.[25]

[22] La norme ISO 27001/27002 est une norme de sécurité mondiale largement adoptée qui définit les exigences et les bonnes pratiques pour une approche systématique de la gestion des informations sur les entreprises et les clients basées sur des évaluations périodiques des risques adaptées à des scénarios de menaces en constante évolution. La norme ISO 27018 est un code de pratique qui se concentre sur la protection des données personnelles dans le cloud. Elle est basée sur la norme ISO de sécurité de l'information 27002 et fournit des conseils d'application sur les contrôles ISO 27002 applicables aux informations personnelles identifiables (PII) dans le cloud public. Elle fournit également un ensemble de contrôles supplémentaires et des conseils connexes destinés à répondre aux exigences de protection des PII dans le cloud public qui ne sont pas prises en compte par l'ensemble de contrôles existant grâce à la norme ISO 27002.

[23] La norme PCI DSS (Payment Card Industry Data Security Standard) est une norme exclusive de sécurité des informations propriétaires administrée par le Conseil des normes de sécurité PCI (https://fr.pcisecuritystandards.org/minisite/env2/), fondée par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. La norme PCI DSS s'applique à toutes les entités qui stockent, traitent ou transmettent des données de titulaires de carte (CHD) et/ou des données d'authentification sensibles (SAD), y compris les commerçants, les personnes réalisant des traitements, les acquéreurs, les émetteurs et les fournisseurs de services.

[24] Les rapports SOC (SOC 1, 2, 3) visent à répondre à un large éventail d'exigences en matière d'audit financier pour les organismes d'audit américains et internationaux. L'audit de ce rapport est effectué conformément aux Normes internationales de missions d'assurance n° 3402 (ISAE 3402) et à l'Institut américain des experts comptables (AICPA) : AT 801 (anciennement SSAE 16).

[25] Voir https://aws.amazon.com/fr/compliance/services-in-scope/.