agora

Sécurité Papier blanc

agora.io

Contenu

Introduction

Agora s'engage à fournir aux développeurs une plate-forme d'engagement en temps réel (RTE) omniprésente en tant que service (PaaS) - permettant à chacun d'interagir avec n'importe qui, n'importe quand, n'importe où. Agora a conçu un réseau mondial propriétaire pour la transmission et l'interaction audio et vidéo - nous l'appelons SD-RTN™ (Software Defined Real-time Network). En conjonction avec notre SD-RTN™, Agora fournit des solutions API et SDK unifiées et standardisées pour divers secteurs et cas d'utilisation sur de nombreux systèmes d'exploitation et plates-formes populaires. Les développeurs peuvent facilement créer des expériences RTE sûres, fiables et de haute qualité en intégrant le SDK Agora dans leurs systèmes ou applications pour ajouter des fonctionnalités telles que les appels vidéo et vocaux, la messagerie en temps réel, l'enregistrement et la diffusion interactive en direct.

En tant que pionnier de l'industrie et premier fournisseur de services RTE au monde, la sécurité de l'information, la conformité légale et la confidentialité des données sont les principales priorités organisationnelles d'Agora. La confidentialité des données dès la conception et par défaut sont des considérations essentielles lors de la création de capacités RTE. L'objectif de ce document est de décrire les e orts d'Agora et les attributs de la plate-forme en matière de sécurité, de conformité et de confidentialité, afin que les développeurs puissent utiliser le service Agora RTE en toute tranquillité.

Dans cet article, nous explorerons systématiquement les attributs de la plate-forme Agora RTE et les e orts de l'entreprise en matière de sécurité, de conformité, de confidentialité et de traitement des données.

1. Responsabilité partagée de la sécurité

Agora s'appuie sur la coopération des clients dans un effort commun pour améliorer en permanence la sécurité.

Afin d'aider les développeurs à comprendre les responsabilités en matière de sécurité dans des scénarios RTE complexes, nous avons créé ce modèle de partage :

Modèle de partage des responsabilités en matière de sécurité

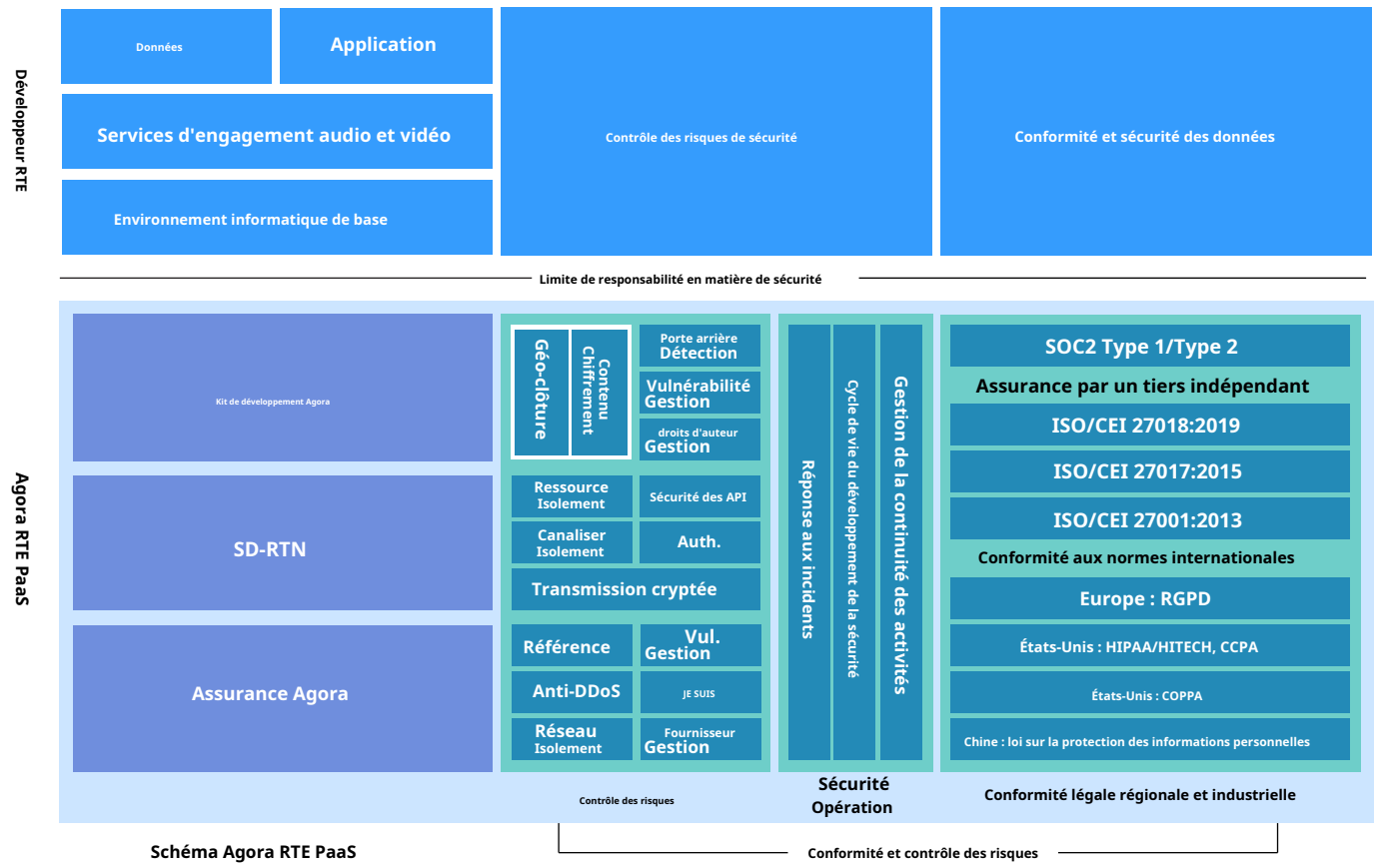

Schéma Agora RTE PaaS

Agora gère et contrôle la sécurité de notre plateforme RTE (PaaS) et SDK. Les clients doivent gérer et contrôler la sécurité de leurs propres applications et environnements système. De plus, en fonction de leurs propres besoins, les clients doivent configurer correctement les paramètres de sécurité du SDK Agora pour assurer la sécurité de leurs propres informations, plateforme, programme, système et réseau.

2. Conformité à la sécurité et protection de la vie privée

La conformité et la protection de la vie privée sont des priorités absolues du service Agora RTE. Agora s'engage à offrir une plate-forme toujours conforme aux réglementations nationales et étrangères en matière de confidentialité, notamment le RGPD de l'Union européenne, le CCPA des États-Unis, la HIPAA, la COPPA et la loi chinoise sur la protection des informations personnelles.

Au service des objectifs ci-dessus, nous avons mis en place des équipes dédiées à la confidentialité, à la conformité et à la sécurité des informations qui ont élaboré une série de politiques, de flux de travail et de systèmes utilisés pour protéger les informations personnelles des clients. Pour garantir que la confidentialité et la sécurité sont implicites par défaut, nous adhérons aux principes de confidentialité dès la conception (PbD) et tous les produits sont soumis à une évaluation de sécurité rigoureuse. Nous traitons toutes les données personnelles en stricte conformité avec les lois sur la protection de la vie privée du pays et/ou de la région.

Agora utilise également des mesures techniques pour protéger les informations personnelles des clients et éviter l'accès non autorisé, la modification, la divulgation et/ou l'abus des informations personnelles. Notre SDK voix et vidéo fournit un algorithme de cryptage intégré, et la communication réseau avec les clients (via notre SD-RTN™) est protégée par un protocole de transmission crypté. Agora ne lit aucun contenu crypté ni ne l'associe à un client spécifique.

Nous nous engageons à utiliser les normes internationales et les meilleures pratiques dans l'évolution continue de notre système de gestion de la sécurité. En plus d'assurer la sécurité et la conformité de nos propres produits, nous fournissons une assistance en matière de conformité à nos clients, afin de les aider à se conformer aux lois et aux exigences réglementaires applicables.

Agora a non seulement obtenu une série de certifications de systèmes de gestion de la sécurité des informations et de la confidentialité internationalement reconnues (dont ISO/IEC 27001, ISO/IEC ISO27017 et ISO/IEC 27018), mais nous avons également obtenu des certifications SOC2 TYPE II délivrées par un tiers indépendant. commissaire aux comptes du parti. Les tableaux suivants résument ces certifications :

Tableau 1 Certifications ISO

Certificat	Délivré par	Ce que cela signifie pour les clients	Champ d'application
ISO/CEI 27001:2013, Sécurité des informations Système de gestion	DNV	Agora dispose de capacités su isantes d'identification et de contrôle des risques liés à la sécurité de l'information, et nous pouvons fournir des produits et services sûrs et fiables aux clients du monde entier. monde.	• Régions des nœuds RTE d'Agora : Europe, Nord Amérique, Asie, Afrique, Océanie et Sud Amérique. • Clients d'industries : éducation en ligne, pan-divertissement social, jeux interactifs, Santé sur Internet, finance en ligne, commerce électronique, diffusion en direct, vidéo conférence, intelligent matériel, etc • Composants du RTE d'Agora : temps réel produits de fiançailles, modules, systèmes et services (par exemple, SD-RTN™, SDK d'appels vidéo et vocaux, SDK de messagerie en temps réel, SDK d'enregistrement, SDK de diffusion interactive en direct et Argus). • Processus et cycle de vie de la solution Agora RTE et exploitation : Recherche et Développement, Assurance Qualité, Exploitation, Service client, Maintenance technique, Traitement des données, etc
ISO/CEI 27017:2015, Sécurité des informations contrôles applicables à la fourniture et l'utilisation de services cloud	DNV	Les services Agora RTE PaaS disposent de capacités adéquates de gestion et de support de la sécurité de l'information.	
ISO/CEI 27018:2019, Basé sur ISO/CEI 27002, fournit un ensemble d'informations personnellement identifiables (PII) directives de protection et contrôle de sécurité mesures applicables aux clouds publics	DNV	Agora a mis en place une information personnelle système de protection pour protéger les informations personnelles des utilisateurs en termes de confidentialité et de cycle de vie des données. Et nous protégeons les données d'entreprise et les informations personnelles des utilisateurs pour répondre aux normes de pratique reconnues par l'industrie.	

Tableau 2 Rapports SOC2 de l'auditeur de conformité tiers

Certificat	Statut	Ce que cela signifie pour les clients
Type II	Obtenu	• Agora a établi et mis en œuvre un contrôle interne e cace, qui peut garantir de manière continue et e cace la sécurité, la disponibilité, la confidentialité et la confidentialité des différents produits et services. • Agora est régulièrement auditée par des tiers pour vérifier que les produits et services répondent aux normes d'audit.

3. Sécurité de la plateforme Agora RTE

L'interaction en temps réel dépend de garanties de sécurité strictes sur l'ensemble de la plate-forme RTE. Dans l'environnement Internet, ces garanties de sécurité sont nécessaires pour maintenir les services disponibles et protéger les données des clients.

Alors que nous continuons à faire évoluer notre offre de services RTE, nous nous engageons à évaluer en permanence les risques techniques liés à l'architecture de la plateforme et avons pleinement intégré le contrôle des risques de sécurité et la conformité aux normes dans tous les aspects de la construction, de la mise en œuvre et de l'exploitation de la plateforme.

La plate-forme Agora RTE est principalement composée de l'infrastructure ultérieure, du SD-RTN™ et du SDK Agora. Dans cette section, nous discutons des mesures de contrôle des risques de sécurité associées à chaque couche de technologie et d'opérations.

3.1 Sécurité de la couche infrastructure

L'infrastructure Agora est composée de plus de deux cents centres de données Internet (IDC) privés, stratégiquement situés, fonctionnant en combinaison avec les services de cloud public virtuel (VPC) des principaux fournisseurs de cloud public, pour fournir un environnement informatique unifié hautement disponible et évolutif. , efficace et sécurisé.

3.1.1 Gestion de la sécurité des appareils dans les IDC privés

La gestion quotidienne des appareils dans nos IDC privés est coordonnée et prise en charge par les opérateurs de centres de données confiés. Conformément aux exigences du service RTE, Agora a formulé un cahier des charges complet de gestion des fournisseurs de datacenters. Le cahier des charges définit les modes de gestion et les normes de mise en œuvre des services que les fournisseurs doivent respecter. En bref, les fournisseurs sont responsables de la sécurité de l'environnement physique, de la protection de l'alimentation, de l'inspection quotidienne, de la commutation de redondance physique, de la surveillance et des rapports anormaux, etc.

Nous sélectionnons uniquement des fournisseurs ayant obtenu la certification ISO27001 ou équivalente/supérieure et nous confirmons qu'ils répondent à toutes les exigences de sécurité d'Agora dans ces domaines :

- Gestion des accès
- Gestion des risques
- Réponse aux incidents
- Sécurité Internet
- Surveillance des alertes
- Reprise après sinistre

Avant de mettre nos appareils IDC en service, nous effectuons un processus d'initialisation unifié. Lors de l'exécution de ces appareils, nous collectons des données relatives à l'état de fonctionnement en temps réel, telles que la charge du système d'exploitation et le flux réseau. Nous configurons également des alertes d'incidents de service sur notre plateforme de surveillance. En cas d'alerte, une équipe opérationnelle Agora 24h/24 et 7j/7 y répondra, traitera les exceptions et rétablira rapidement le service. Avant que les appareils ne soient mis hors ligne, nous mettons en œuvre un traitement de cryptage des données, puis les fournisseurs sont chargés de les expédier à l'environnement de traitement centralisé d'Agora. Comme dernière étape, nous scellerons ou effectuerons une destruction physique après avoir effacé les données et les configurations.

3.1.2 Isolement du réseau

L'une des conditions préalables à la sécurité du réseau est une isolation efficace du réseau. Sur la base des di érences dans les fonctions de la plate-forme RTE, nous divisons le réseau en plusieurs groupes de sécurité, notamment Core, Edge et IT. Dans chacun de ces groupes, di érentes règles de routage et d'accès strictes sont mises en œuvre en fonction des exigences de service et des niveaux de sécurité. Pour obtenir une capacité d'isolation réseau unifiée, nous programmons les règles de sécurité réseau directement dans notre commutateur matériel réseau dans nos IDC privés pour donner une couche de sécurité supplémentaire. Nous complétons ces règles sur le commutateur dans nos IDC privés basés sur le groupe de sécurité du cloud privé virtuel (VPC) tandis que dans le cloud public

3.1.3 Anti-DDoS

Les attaques par déni de service distribué (DDoS) peuvent avoir un impact significatif sur les services de RTE, notamment une dégradation de la qualité ou, dans certains cas, une interruption de service. Pour assurer la disponibilité de la plateforme Agora RTE, nous avons déployé une solution de défense DDoS pour nos services de base via les capacités des fournisseurs de cloud public. La solution peut détecter automatiquement une attaque, puis programmer et appeler la fonction d'atténuation DDoS, qui peut être exécutée en quelques secondes. L'équipe de sécurité Agora 24h/24 et 7j/7 est informée de toute attaque DDoS afin qu'elle puisse surveiller et prendre la meilleure décision de réponse.

3.1.4 Sécurité de l'hôte, de la base de données et du middleware

Les services en fonctionnement dépendent de la garantie des ressources informatiques - programmes d'arrière-plan, caches, bases de données et autres logiciels intermédiaires. Cette garantie est satisfaite par une planification et une allocation rationnelles du CPU, de la mémoire, du disque, etc., via le fonctionnement du système ou le conteneur.

3.1.4.1 Renforcement de la sécurité

Nous avons formulé une série de lignes de base de sécurité pour nos IDC et VPC privés qui couvrent les systèmes d'exploitation, les conteneurs, les bases de données, le stockage, les services Web, etc. Ces lignes de base traitent de la sécurité des comptes, de l'identité, de l'authentification, de l'autorisation minimale, de l'audit des journaux et de la synchronisation de l'horloge. En pratique, nous mettons en œuvre un renforcement de la sécurité sur ces lignes de base en fonction d'un certain nombre de facteurs, notamment le type d'appareil ou de service, le niveau d'actif et l'utilisation, afin de garantir que nos ressources informatiques répondent à nos exigences de sécurité. Nous effectuons également des inspections régulières de la configuration des ressources et comparons avec les lignes de base pour identifier les vulnérabilités potentielles. Si des vulnérabilités sont détectées, l'équipe des opérations de sécurité informe les équipes commerciales, techniques ou opérationnelles associées pour mettre en œuvre les modifications nécessaires.

3.1.4.2 Gestion des vulnérabilités

Toutes les ressources informatiques d'Agora sont soigneusement analysées pour les vulnérabilités de sécurité. Nous collectons les informations de version des composants dans le système d'exploitation de la sécurité pour une analyse centralisée afin d'identifier si un package ou un service est affecté par des vulnérabilités connues. Comme pour les hôtes sur le cloud public, des agents de sécurité sont également déployés pour détecter les vulnérabilités en temps réel. De plus, l'équipe de sécurité analyse régulièrement les actifs à la fois dans nos IDC et dans nos VPC sur les clouds publics, examine les rapports et consigne les problèmes dans le système de gestion des incidents et des événements de sécurité. Si une vulnérabilité est identifiée, l'équipe de sécurité fournit une évaluation complète du risque, en proposant des mesures de traitement et des suggestions de correctifs. L'équipe de sécurité travaille avec les commerciaux, les techniciens et les opérationnels

équipes pour effectuer les réparations nécessaires, le renforcement de la sécurité et la mise à jour des images.

3.1.4.3 Sécurité Exploitation des Infrastructures

Opération Sécurité du compte

Dans l'exploitation et la maintenance quotidiennes, nous avons mis en place un mécanisme de gestion des identités et des accès (IAM). L'identité de tous les opérateurs doit être vérifiée et autorisée avant qu'ils puissent effectuer des modifications du système. De plus, ces comptes sont corrélés aux identités des employés des équipes opérationnelles et l'authentification multifacteur (MFA) est activée par défaut.

Nous avons également créé un ensemble de contrôles stricts pour l'utilisation des API de service de cloud public. Les programmes ne sont accessibles que via une clé d'accès autorisée ou des informations d'identification de rôle assumé. Les mots de passe ou les clés d'accès associés au compte root ne sont pas autorisés.

Sécurité du compte du système d'exploitation

La sécurité des comptes du système d'exploitation comprend l'utilisation de mots de passe forts avec une rotation régulière et l'équipe de sécurité effectue des inspections régulières.

Audit des opérations

Nous enregistrons et archivons tous les processus d'exploitation et de maintenance en temps réel. Des politiques et des métriques sont en place qui déclenchent une alarme dès qu'une opération à risque est détectée.

3.2 Sécurité SD-RTN™

Le SD-RTN™ d'Agora, le plus grand réseau en temps réel défini par logiciel au monde, est spécialisé dans l'interaction audio et vidéo en temps réel. Ses principaux avantages sont une latence ultra-faible, une transmission de haute qualité et la prise en charge de millions d'utilisateurs, qui interagissent en temps réel. En tant que l'un des services de base de la plate-forme Agora RTE, SD-RTN™ prend en charge l'accès à la source du terminal RTE, l'authentification, l'autorisation, le routage intelligent, la planification en temps réel et la transmission en temps réel.

Afin d'assurer la conformité et la sécurité des services de RTE, nous avons construit l'architecture de SD-RTN™ en tenant compte des menaces Internet. SD-RTN™ fournit aux clients des services sécurisés et stables grâce aux mesures de contrôle suivantes :

3.2.1 Isolement des ressources

SD-RTN™ alloue des ressources dédiées à chaque projet RTE pour s'assurer qu'il est indépendant des autres ressources du projet, et SD-RTN™ fournit des ressources sécurisées et fiables pour l'accès, le calcul et la transmission. Les clients n'ont qu'à effectuer une configuration simple sur la console client Agora. Lorsqu'un projet RTE est créé par un client, nous attribuons automatiquement un identifiant d'application unique au projet et nous attribuons le

Ressources associées. Simultanément, le SD-RTN™ isole les ressources en fonction de l'ID de l'application.

3.2.2 Isolation des canaux

Nous créons un canal indépendant et isolé pour chaque type de transmission de données audio, vidéo ou message. Tous les canaux sont logiquement séparés ; seuls les utilisateurs ayant le même ID d'application pour les applications interactives audio et vidéo et le même nom de canal peuvent rejoindre un canal donné. Lorsqu'un utilisateur démarre une session, le canal est créé. Lorsque la session se termine (le dernier utilisateur quitte), le canal est détruit.

3.2.3 Transmission cryptée

Afin d'assurer la confidentialité du processus de transmission, le SD-RTN™ utilise Agora Universal Transport (AUT). (un protocole de transmission personnalisé basé sur TLS 1.3) pour apporter des garanties de chiffrement sur les liens de transmission de RTE. AUT est globalement activé, par défaut, sur la plateforme Agora RTE.

3.2.4 Authentification

Lorsque les utilisateurs de l'application RTE accèdent à la plateforme Agora RTE, nous fournissons un service de génération de jetons dynamiques basés sur l'App ID. avec le certificat d'application pour l'authentification, afin d'aider les clients à effectuer une authentification forte sur leurs utilisateurs en cas de besoin. Pour utiliser le service d'authentification dynamique, les clients doivent d'abord le configurer dans la console.

Pour plus d'informations, consultez "Meilleures pratiques de sécurité" à l'adresse https://docs.agora.io/en/Agora%20Platform/security_practice?platform=All%20Platforms.

3.3 Sécurité du SDK

Agora fournit la prise en charge du SDK RTE pour des plates-formes telles qu'iOS, Android, macOS, Windows, Linux, les applets et le Web, afin de répondre aux besoins d'engagement en temps réel des clients dans diverses circonstances. Le SDK Agora RTE fournit non seulement aux clients un kit de développement simple, facile à utiliser, unifié, crédible et sécurisé, mais il fournit également aux clients des options de configuration conformes et sécurisées. L'objectif est d'optimiser les scénarios d'engagement en temps réel des clients de manière conforme avec la capacité d'identifier rapidement et de répondre complètement à toute menace contre les données sources.

3.3.1 Fonctionnalités de sécurité du SDK

Lorsqu'Agora fournit des SDK à ses clients, la sécurité est l'une de nos principales garanties. Lors de l'ajout de fonctionnalités ou de l'itération de versions d'un SDK, Agora évalue entièrement les points de risque des exigences fonctionnelles, en termes de conformité, de confidentialité et de sécurité. Tous les codes

est soigneusement audité rigoureusement testé pour l'assurance qualité. Lorsqu'un code tiers cité ou intégré est intégré, Agora évalue minutieusement les rapports de tests d'intrusion à la recherche de code malveillant ou de portes dérobées. Nous garantissons également le respect des droits d'auteur et des accords d'utilisation. Si des risques sont détectés, le processus de publication est suspendu jusqu'à ce que toutes les vulnérabilités aient été corrigées et que tous les bogues aient été corrigés.

3.3.2 Cryptage du contenu et géolocalisation

Afin d'aider nos clients à améliorer la sécurité, la conformité et la confidentialité des données dans les scénarios RTE, Agora fournit des options de cryptage des sources de données et de géolocalisation.

3.3.2.1 Chiffrement du contenu

Le SDK Agora prend en charge le chiffrement au niveau des données de tous les flux audio, flux vidéo et messagerie à l'aide d'algorithmes de chiffrement symétrique AES 128/256. Les données cryptées sont transmises aux autres nœuds du canal via l'Agora SD-RTN™. À l'extrémité de réception, il est déchiffré par l'application, puis transmis au moteur de rendu du flux multimédia. La clé de chiffrement n'est connue que du développeur de l'application et n'est pas envoyée au serveur Agora.

3.3.2.2 Géolocalisation du réseau

Afin de répondre aux exigences légales et réglementaires des di érents pays ou régions, la plate-forme Agora prend en charge la géolocalisation du réseau afin que les clients aient un contrôle total sur les pays et régions où leurs données pourraient transiter. Les clients peuvent configurer et activer la géolocalisation dans le SDK en fonction de leurs besoins.

Se référer à la documentation de développementici pour activer ces fonctions dans leurs configurations.

3.4 Sécurité des API Web

Les clients gèrent leurs projets et canaux en appelant les API RESTful de la console sur la plateforme Agora RTE, Cette documentation est disponible sur https://docs.agora.io/en/rtc/restfulapi/

Pour protéger les API, nous utilisons non seulement des solutions WAF, mais mettons également en œuvre les mesures de contrôle suivantes :

3.4.1 Authentification d'identité

Avant d'utiliser l'API Agora RESTful, les clients doivent se connecter à la console Agora (https://console.agora.io/) et créer une paire clé et secret. Les appels d'API suivants nécessitent la paire clé-secret correspondante. Cela garantit une séparation sécurisée des di érents

projets et candidatures.

3.4.2 Sécurité des transmissions

Les API reposantes ne prennent en charge que le protocole HTTPS garantissant que toutes les communications sont cryptées avec SSL/TLS, protégeant à la fois les informations d'identification de l'API et les données transmises. Cela fonctionne également pour empêcher l'homme du milieu et d'autres attaques.

3.4.3 Limite QPS des appels API

Les requêtes par seconde (RPS) des appels d'API sont limitées afin de garantir qu'il est possible de répondre aux demandes normales des utilisateurs et de refuser les utilisateurs malveillants.

3.4.4 Vérification des entrées

Pour éviter les failles de vulnérabilité courantes (injection SQL, exécution de code à distance, etc.), les paramètres demandés par les appels utilisateurs sont vérifiés et filtrés par le serveur.

3.4.5 Encodage de sortie

Le serveur ajoute des options de sécurité (Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, etc.) aux en-têtes des réponses pour augmenter la protection.

4. Sécurité des données

Il est important de traiter les données de manière légale, conforme et sécurisée, et c'est l'une de nos principales préoccupations. Cette section décrit nos politiques sur la sécurité et la gestion des données, ainsi que les mesures de contrôle technique en place pour les soutenir.

4.1 Organisation de la sécurité des données

Nous avons mis en place un comité de sécurité et de confidentialité des données (DSPC) pour se concentrer sur les politiques de sécurité des données et de protection de la vie privée de notre plateforme et de nos services. Ce comité supervise la mise en œuvre des politiques, procédures et précautions, et est chargé de traiter rapidement tout problème de technologie de sécurité des données et de respect de la vie privée. La DSPC est composée de personnels issus des équipes et des directions de la Sécurité, des A aires Juridiques, de la plateforme de données et de la direction. De plus, nous avons un responsable de la protection des données (DPO) responsable de la classification des données, du respect de la confidentialité et de la protection.

4.2 Politique de sécurité des données

En réponse à la sévérité croissante des menaces à la sécurité des réseaux et au resserrement progressif

des exigences réglementaires, nous avons intégré la sécurité des données dans le processus de construction du système de sécurité, en nous concentrant sur :

• Confidentialité : pour empêcher l'accès non autorisé et l'écoute clandestine
• Intégrité : pour empêcher la falsification malveillante et la falsification des données
• Disponibilité : SD-RTN™ prend en charge la haute disponibilité des données

De plus, tous les employés d'Agora :

• Signer des accords de confidentialité
• Suivre une formation régulière sur la protection des informations, le respect de la vie privée et la sensibilisation à la confidentialité

De plus, tous les employés ayant accès aux systèmes ou aux données de la plate-forme reçoivent une formation avancée en matière de sécurité organisée par le centre de support du système d'information, qui est responsable du fonctionnement et de la maintenance normaux de la plate-forme d'exploitation et des services.

4.3 Collecte de données

Nous adoptons le principe de la collecte minimale de données et ne collectons que les champs de données qui sont 1) nécessaires à la conduite des affaires et 2) autorisés et acceptés par le client. Les données utilisateur collectées par les clients Agora, telles que les identifiants de connexion et les informations de paiement, sont entièrement gérées par les clients Agora eux-mêmes. Ces informations utilisateur ne sont pas stockées sur la plateforme Agora.

4.4 Masquage des données

Afin de protéger la confidentialité des données, nous n'affichons que des informations d'entreprise et personnelles désensibilisées dans la console Agora. Cette stratégie est également applicable sur l'ensemble de la plate-forme en interne, y compris la plate-forme de gestion interne d'Agora, l'impression des journaux, la surveillance des alarmes et tous les autres endroits où les données sont affichées.

4.5 Protection des données et cryptage de la transmission

La protection des données est au cœur de la stratégie de sécurité d'Agora RTE. Au sein de notre plateforme RTE, SD-RTN™ o re une sécurité supplémentaire des données, vous pouvez trouver des informations plus détaillées dans "3.2 SD-RTN™ Security". Pour les solutions qui ne reposent pas sur SD-RTN™ (telles que le SDK Web, l'enregistrement dans le cloud, l'approbation du contenu et le transcodage), nous proposons une méthode de chiffrement di érente.
Dans ces cas, le chiffrement est géré par le standard WebRTC et l'interopérabilité avec Agora est réalisée grâce à notre moteur de chiffrement (la clé a été transférée en toute sécurité sur le serveur Web SDK via l'API). Pour plus d'informations sur la sécurité WebRTC, consultez

https://webrtc-security.github.io.

4.6 Utilisation et stockage des données

Nous séparons strictement les environnements de production, de test et de développement. Les données réelles ne sont pas utilisées pour le développement ou les tests. En production, si un client utilise les fonctionnalités d'enregistrement fournies par la plateforme Agora, ces enregistrements sont toujours stockés sur les serveurs du client et jamais stockés sur les serveurs Agora.

En ce qui concerne les informations stockées, nous établissons des politiques de sauvegarde et de stockage des données conformément aux exigences réglementaires applicables. Lors du traitement des demandes des clients, nous coopérerons à la mise en œuvre du nettoyage ou du transfert des données conformément aux exigences réglementaires correspondantes autorisées par les clients. Pour plus de détails sur la collecte et l'utilisation des données d'Agora, consultez notre politique de confidentialité (https://www.agora.io/en/privacy-policy/) et consignes de sécurité des informations (https://docs.agora.io/en/Agora%20Platform/security?platform=All%20Platforms).

4.7 Haute disponibilité du service de données

Les clients qui utilisent le réseau d'Agora (SD-RTN) bénéficient de services de données RTE hautement disponibles qui incluent ces fonctionnalités :

• Centres de données de masse : plusieurs centres de données sont déployés dans le monde pour fournir des services, et toute attaque de centre de données n'affectera pas le fonctionnement normal des autres nœuds de données, garantissant ainsi la stabilité du service global.

• Autoréparation des pannes : si le serveur tombe en panne en raison d'attaques malveillantes, telles que le déni de service (DoS), nous isolons automatiquement la machine défectueuse pour nous assurer que le service n'est pas a ecté.

• Prévention DDoS : nous avons configuré des services anti-DDoS dans chaque centre de données cloud central et nous avons déployé plus de 200 centres de données distribués dans le monde entier pour prévenir et contrôler les risques de sécurité DDoS.

5. Opération de sécurité

La sécurité est un processus continu. Compte tenu des caractéristiques de la plateforme RTE, nous avons développé les opérations de sécurité à travers ces dimensions :

5.1 Cycle de vie du développement de la sécurité

Les exigences liées à la sécurité et à la confidentialité sont indispensables dans notre cycle de vie de développement de logiciels.

Sur la base du cycle de vie du développement de la sécurité (SDLC), nous combinons le concept de DevSecOps avec des méthodes et des outils plus automatiques pour effectuer e iciacement des contrôles de sécurité et de confidentialité.

5.1.1 Modélisation des menaces

Aux étapes de conception et d'architecture, nous utilisons la modélisation des menaces pour identifier les problèmes de sécurité potentiels, puis nous mettons en œuvre des mesures de réponse conçues pour détecter ces risques plus tôt. Pour identifier et résoudre efficacement les risques, nous nous référons à la méthode de modélisation des menaces STRIDE et nous concentrons sur la minimisation de la surface d'attaque, la confidentialité de base, la minimisation des autorisations, la sécurité par défaut et le cryptage des données.

5.1.2 Détection des boîtes noires et des boîtes blanches CI/CD

Lors de la phase de test, nous accordons une attention particulière aux mécanismes de protection de sécurité intégrés préconisés par DevSecOps. Pour améliorer notre capacité de détection des risques, nous avons intégré des outils de test de boîte noire et de boîte blanche aux étapes CI/CD, notamment SonarQube (un outil d'analyse de code open source), Black Duck (un composant commercial et un outil d'analyse de conformité) et MobSF (et framework de sécurité mobile open source).

5.2 Anti-intrusion et moniteur de sécurité

Afin de mettre en place une défense en profondeur pour répondre aux menaces, nous collectons des logs pour analyse de sécurité (dans le cadre d'une autorité minimale). Ces journaux sont utilisés par notre plateforme de surveillance et d'analyse de la sécurité en temps réel. Lorsqu'un événement anormal est détecté, nous alertons l'équipe des opérations de sécurité et lui demandons d'étendre l'analyse de corrélation et de traçabilité. Si un incident est confirmé, il est traité selon le mécanisme d'intervention d'urgence. L'équipe continue de surveiller pour assurer la sécurité et la disponibilité des systèmes de l'entreprise.

5.3 Planification et intervention d'urgence

Conformément aux caractéristiques des prestations de RTE, nous avons classé et gradué les types de prestations et formulé di érentes normes de classification des incidents en identifiant systématiquement les menaces et en évaluant les risques. Dans le même temps, des délais de réponse et des procédures de traitement adaptés sont mis en œuvre pour garantir que les incidents sont traités de manière rapide et efficace. En bref, notre processus de réponse est le suivant :

Détection d'anomalies → Confirmation d'incident → Suppression d'événement → Gestion des événements → Analyse de la cause fondamentale → Rapport final

5.4 Gestion de la continuité des activités

Une faible latence et une haute qualité nécessitent une haute disponibilité de la plateforme Agora RTE. Pour nous assurer de pouvoir fournir des services RTE continus (24h/24 et 7j/7) aux clients, nous avons mis en place une équipe professionnelle et e iciace responsable du support et de la gestion de la continuité.

5.4.1 Surveillance en temps réel

Nous avons construit un ensemble d'outils de surveillance unifiés pour inspecter l'état et le niveau de ressources des composants du système, y compris le middleware, la charge informatique, les bases de données et les périphériques réseau, pour chaque service. Dès qu'une exception se produit, des alarmes automatiques déclenchent des robots de messages pour informer les équipes d'astreinte de rétablir les services et d'assurer la disponibilité.

Nous maintenons également un affichage centralisé et quantitatif des principaux indicateurs de service qui nous permet de surveiller la situation globale du service en temps réel. Cela améliore notre capacité à prendre des décisions d'expansion opportunes et raisonnables sur l'utilisation des ressources de l'entreprise.

5.4.2 Reprise après sinistre et redondance

Lors de la conception de l'infrastructure de la plate-forme RTE, nous avons envisagé des scénarios de charge informatique extrême et intégré la redondance appropriée dans nos centres de données Internet. Pour garantir la disponibilité de nos ressources de base en cas d'urgence, nous avons combiné nos IDC avec les principaux services de cloud public. Le modèle de cloud hybride est une mesure importante pour la haute disponibilité de l'Agora RTE PaaS.

5.4.3 Exercices de continuité

Pour assurer la continuité et le bon fonctionnement des services les plus importants de RTE, nous réalisons régulièrement des exercices d'urgence sur le réseau, les charges de calcul, le middleware, les systèmes métiers, etc. Nous examinons et analysons les résultats et les données de chaque exercice pour aider à la optimisation des architectures techniques, des processus et des plans d'urgence.

6. Culture de sécurité

La sécurité de l'information est un projet systématique qui nécessite non seulement le soutien du niveau stratégique de l'entreprise, mais également la participation de tous les employés. En fin de compte, la sécurité des informations dépend de la coopération des clients, des organisations tierces et des individus de l'écosystème de l'industrie. Agora intègre pleinement cette compréhension dans les opérations quotidiennes et les processus de gestion.

6.1 Organisation de la sécurité

Nous avons pleinement reconnu la position stratégique de la sécurité de l'information et son rôle de soutien dans le développement commercial à long terme de l'entreprise, et nous avons constitué une équipe indépendante de sécurité de l'information qui sera responsable de la construction et de l'amélioration des capacités de sécurité d'Agora. Nous avons également mis en place ces organisations internes virtuelles :

- Équipe de gestion de la sécurité de l'information
- Équipe de conformité de sécurité et de confidentialité
- Équipe de contrôle interne de la sécurité
- Équipe de sécurité des données

Ces équipes travaillent sur les aspects techniques, de gestion et juridiques pour s'assurer que la sécurité de l'information peut être coordonnée à l'échelle mondiale (à partir du niveau stratégique) et que les politiques de sécurité peuvent être e cacement transmis, étape par étape, pour s'assurer que les mesures de sécurité sont mises en œuvre.

6.2 Sécurité des employés

Agora attache une grande importance aux contributions des employés à notre produit, à notre culture et à notre succès, et en tant qu'élément essentiel de nos e orts de sécurité. Pour garantir que les employés partagent les valeurs et l'éthique d'Agora tout en répondant aux exigences de sécurité de l'information, nous avons intégré la sécurité et l'éthique à chaque étape du cycle de vie des employés, du recrutement et de l'intégration à la formation et à la démission.

6.2.1 Recrutement

Les candidats sont examinés professionnellement par un organisme de vérification des antécédents avant d'être embauchés. Nous vérifions l'éducation, les emplois précédents, les références externes, les casiers judiciaires, la cote de crédit, le statut d'immigration et d'autres informations lorsque les lois du travail locales ou les réglementations statutaires le permettent.

6.2.2 Intégration

Notre processus d'intégration des nouveaux employés met l'accent sur le Code de conduite des employés et sur la compréhension des exigences de notre gestion de la sécurité de l'information. Selon les exigences du poste, nous pouvons signer des accords de confidentialité. Les employés occupant des postes impliquant des données importantes ou des informations sur les consommateurs sont tenus de signer le plus haut niveau d'accord de confidentialité et nous nous assurons qu'ils comprennent parfaitement les responsabilités en matière de sécurité.

6.2.3 Au travail

Les employés au travail sont tenus de participer à une formation en ligne de sensibilisation à la sécurité et à la protection de la vie privée. Cette formation comprend GDPR, HIPAA et d'autres lois et réglementations ainsi qu'une sensibilisation quotidienne à la sécurité des bureaux. Les employés doivent réussir des examens. De plus, Agora organise périodiquement des événements éducatifs liés à la sécurité et à la confidentialité.

6.2.4 Démission

Les employés qui ont démissionné doivent céder ou fermer leurs droits d'accès physiques et logiques conformément au processus de démission établi. Nous auditerons l'exécution de la période de confidentialité conformément à l'accord de confidentialité signé par les employés, et nous les informerons clairement de leur responsabilité postérieure à l'emploi en matière de sécurité et de confidentialité des informations. Les employés occupant des postes clés doivent signer des accords de non-concurrence, le cas échéant, lors de leur embauche. Le processus de démission nécessite un transfert de travail, le nettoyage des données et la réussite d'un audit.

6.3 Collaboration en matière de sécurité avec des ressources externes

Notre objectif est de fournir aux clients et aux développeurs une plateforme de services RTE sécurisée et fiable. À cette fin, nous travaillons également avec des fournisseurs de sécurité tiers, tels que Trustwave et BishopFox, pour effectuer des tests de pénétration externes, des révisions de code et de l'ingénierie inverse. Ces ressources renforcent notre capacité à identifier les vulnérabilités et les risques, améliorant ainsi la sécurité globale des services d'Agora et la robustesse du système.

Nous attachons également une grande importance aux commentaires des clients, des communautés de recherche en sécurité, des équipes white hat, etc. Nous avons créé le programme Agora Bug Bounty pour recevoir des commentaires sur les vulnérabilités de sécurité potentielles et/ou les risques de sécurité. Pour en savoir plus sur le programme Bug Bounty, visitez cette page :https://docs.agora.io/en/Agora%20Platform/bug_bounty

Toutes les vulnérabilités, suggestions, etc. liées à la sécurité peuvent également nous être soumises via cette adresse :security@agora.io

Résumé

L'objectif d'Agora de fournir aux clients et aux développeurs une plate-forme RTE conforme, hautement sécurisée et hautement fiable, est à la base de notre culture d'entreprise et sous-tend toutes les prises de décision liées à notre architecture, nos produits et notre offre de services. A cette fin, Agora :

- Favorise systématiquement la mise en œuvre de politiques de sécurité de l'information liées au personnel, à la technologie et aux processus de gestion.
- Satisfait à toutes les obligations de conformité réglementaire, y compris les normes de sécurité ISO/IEC 27001, 27017, 27018 et SOC 2 et les réglementations de confidentialité telles que GDPR, CCPA et HIPAA.
- Travaille en étroite collaboration avec des partenaires, des clients et d'autres parties pour rester à la pointe des capacités de protection de sécurité intelligentes et hautement efficaces.

Dans un environnement Internet de plus en plus complexe, avec de nouvelles menaces qui émergent chaque jour, il est essentiel de choisir une plateforme RTE capable d'assurer la sécurité et la confidentialité de votre entreprise et de vos utilisateurs. Agora s'engage à assurer la continuité des services de RTE tout en défendant les droits légitimes et la vie privée de tous les utilisateurs finaux de RTE.