RingCentral

FR

Votre guide ultime pour la sécurité des communications cloud

Les conditions essentielles en matière de sécurité, de protection des données et de conformité pour une plateforme UCaaS fiable.

Table des matières

Introduction 3

Les essentiels en matière de sécurité UCaaS : les 3 axes pour une plateforme fiable 6

RingCentral : une approche de premier plan pour une solution UCaaS de confiance 9

Approfondissement : protection de la sécurité des informations + gestion de la confidentialité des données et de la conformité 11

- Sécurité physique 12
- Sécurité du réseau 12
- Chiffrement des données 13
- Prévention des fraudes 13
- Réaction en cas d'incident 14
- Données protégées 14
- Sécurité des opérations 14
- Gestion des fournisseurs 15
- Traitement des données 15
- Cycle de développement logiciel 15

Approfondissement : certifications et attestations en matière de protection des données et de sécurité 16

Approfondissement : contrôles de la politique de sécurité et d'administration 18

- Vidéo 18
- Téléphonie 19
- Messagerie 20
- Accès et identité 20
- Chiffrement 20
- Application unifiée 20
- Focus sur les innovations : chiffrement de bout en bout pour les appels, la messagerie et les visioconférences 22

Conclusion 24

Introduction

Alors que les plateformes UCaaS (en anglais Unified Communications as a Service, ou Communications Unifiées en tant que Service) jouent le rôle d'accélérateurs d'innovation et favorisent le partage de ressources via différents canaux tels que le chat, la voix et la collaboration vidéo, il est crucial pour les entreprises d'examiner avec soin la façon dont le fournisseur UCaaS qu'elles ont choisi gère les questions de sécurité, de protection des données et de conformité afin d'endiguer l'augmentation des menaces majeures qui pèsent sur leur marque et sur leur situation financière.

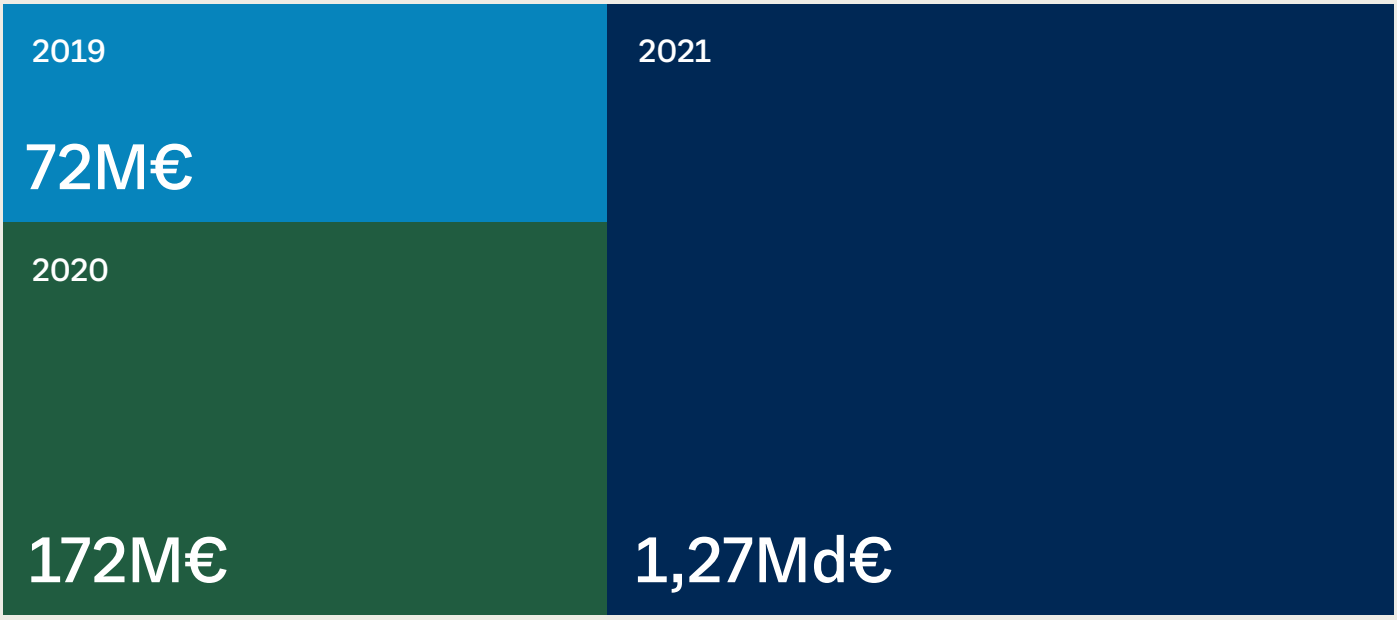
Étant donné que ces menaces augmentent à un rythme record, il est primordial pour les entreprises de s'assurer que la plateforme UCaaS qu'elles souhaitent acquérir offre une approche avant-gardiste en matière de réduction des risques.

Le règlement général sur la protection des données (RGPD) et les amendes de plus en plus élevées qui y sont associées mettent en lumière le caractère essentiel d'un examen minutieux des processus et moyens mis en œuvre par votre fournisseur en matière de protection des données. En 2022, rien qu'en France, la CNIL a battu son record de mises en demeure, avec 147 décisions prononcées.

Évaluer de quelle façon un fournisseur UCaaS assurera la protection des données de votre entreprise est un axe majeur, d'autant plus que 62 % des entreprises ne sont pas « totalement en conformité » avec les règles de protection des données qui leur sont imposées, notamment par le RGPD.

1. Enforcementtracker.com. Statistiques chronologiques du nombre et de la somme des amendes infligées dans le cadre du RGPD

Coût annuel des amendes au titre du RGPD en France



L'éventail des menaces s'étend à d'autres domaines que la confidentialité des données et le RGPD. L'infrastructure de sécurité de votre fournisseur UCaaS est, par essence, un élément essentiel de votre stratégie de sécurité.

Votre fournisseur doit être transparent quant aux investissements qu'il a réalisés pour protéger, jour après jour, vos utilisateurs et vos données contre les menaces de sécurité et les pertes de données.

Si la sécurité de votre fournisseur de services UCaaS est défaillante, votre organisation sera plus exposée aux risques de violation de données, qui peuvent nuire à la valeur de votre marque et à votre activité. Le coût moyen d'une violation de données a connu une hausse considérable depuis quelques années, atteignant quelque 4 millions d'euros en 2022, d'après le rapport d'IBM 2022 sur le coût de la violation des données. Les cas de hameçonnage par téléphone représentent quant à eux plus d'un quart du volume total des attaques enregistrées sur le premier trimestre 2022.

Ce guide indique de quelle façon, en mettant en œuvre les contrôles techniques adéquats, une plateforme UCaaS peut être conçue en mettant la sécurité, la confidentialité et la conformité au cœur des investissements en termes d'infrastructure et de stratégie d'innovation.

Ce guide montre également en quoi RingCentral se démarque sur cette question en offrant une plateforme UCaaS de confiance. Leader du Gartner® Magic Quadrant™ en matière de communications unifiées en tant que service pour la huitième année consécutive, RingCentral vous offre la transparence et l'expertise nécessaires pour garantir la protection de vos investissements sur la plateforme UCaaS contre les principales menaces actuelles.

4M€

Coût des violations de données

Augmentation de 12,7 % par rapport à 2020

+550%

Augmentation du nombre d'attaques de vishing entre 2021 et 2022

Selon Agari/PhishLabs

5223€

Coût des interruptions de service par minute

Estimation Gartner IT

2. IBM Security. Rapport sur le coût des violations de données 2022.

Les essentiels en matière de sécurité UCaaS : les 3 axes pour une plateforme fiable

Quels sont les éléments dont vous avez absolument besoin afin de bénéficier de la sécurité, de la confidentialité des données et de la conformité UCaaS adéquates à tout moment ? Et afin d'avoir la certitude que votre plateforme ne présente aucun risque pour votre image de marque et votre activité ?

La combinaison gagnante en matière de sécurité pour votre solution UCaaS doit inclure les axes suivants :

Protection rigoureuse de la sécurité de l'information

Gestion complète de la confidentialité des données et de la conformité

Respect des bonnes pratiques pour les contrôles de la politique de sécurité et d'administration

Par ailleurs, votre confiance en votre plateforme est soutenue par sa fiabilité et sa disponibilité de, qui assurent la continuité de vos activités.

En matière de sécurité des informations, de sécurité du cloud et de protection des données personnelles, les normes ISO/IEC 27001 sont largement reconnues comme des références pour mesurer la sécurité informatique assurée par un fournisseur.

1. Protection de la sécurité de l'information

Au niveau de l'infrastructure, mais aussi du design et des processus utilisés pour la plateforme UCaaS elle-même, votre fournisseur UCaaS doit mettre en place des pratiques de sécurité inviolables et permanentes vous permettant d'avoir la certitude que vos données sont en sécurité.

Votre fournisseur UCaaS doit démontrer qu'il a mis en place les meilleures technologies ainsi que des processus opérationnels rigoureux pour assurer la protection optimale de vos données en continu.

Il doit également fournir des informations détaillées sur les pratiques de sécurité de l'infrastructure cloud de sa plateforme. La protection informatique ne peut pas se bricoler sur le moment, lorsqu'une faille de sécurité devient un problème ; cette approche doit faire partie de l'identité de votre fournisseur et être appliquée à tous les aspects de l'entreprise.

Votre fournisseur doit être prêt à démontrer son fort engagement pour assurer la sécurité des données dans différents domaines, notamment au niveau de la sécurité physique de son environnement, de sa politique en matière de traitement des données et de ses processus d'évaluation régulière de la sécurité.

Vérifiez également si votre fournisseur a obtenu des attestations de conformité et des certifications pouvant témoigner de son engagement en faveur de la sécurité des données, par exemple : Certification SOC 2, C5, Certification ISO 27001, etc.

2. Gestion de la confidentialité des données et de la conformité

Étant donné les nombreuses fonctionnalités offertes par les plateformes UCaaS, il est fort probable que des éléments confidentiels ou des données d'identification soient partagés sur la plateforme, par exemple des plans de produits sensibles, ou des informations sur les clients et sur les employés.

Ce partage facilité, pour une meilleure collaboration, est l'une des grandes valeurs ajoutées des solutions UCaaS. Il est donc logique de s'attendre à ce que votre fournisseur ait mis en place une politique réfléchie de gestion de la confidentialité des données et de la conformité, qui soit appliquée de manière uniforme.

Votre fournisseur doit mettre en place un système complet visant à empêcher la mise en péril accidentelle ou intentionnelle des données protégées, et il doit être transparent sur la manière dont les données sont collectées et utilisées. C'est une condition indispensable pour que vous puissiez avoir confiance dans les pratiques d'un fournisseur en matière de traitement des données, et cela vous permet de vous assurer qu'il respecte la confidentialité des données de votre entreprise.

Votre fournisseur doit avoir mis en place une politique de confidentialité des plus strictes, idéalement documentée dans une déclaration de confidentialité complète et accessible au public. Vérifiez également le niveau de transparence du fournisseur en matière de communication des requêtes reçues au sujet de données des clients, ainsi que les informations précisant comment il a répondu à ces requêtes.

Cela vous permettra d'avoir la certitude que votre fournisseur prend en charge les questions relatives à la réglementation, et d'en être vous-même libéré.

3. Contrôles de la politique de sécurité et d'administration

Des salles d'attente aux mots de passe de réunion, les plateformes UCaaS doivent offrir des fonctions de sécurité complètes afin de protéger la plateforme et de sécuriser l'expérience des utilisateurs. Des options d'administration telles que l'authentification obligatoire pour les participants à une réunion, les contrôles définissant qui peut activer le partage d'écran et le passage obligatoire des participants en salle d'attente avant de les autoriser à rejoindre une réunion permettent de protéger votre entreprise des pertes de données et des personnes mal intentionnées.

En plus de fournir des contrôles approfondis en matière de sécurité et d'application des politiques, votre plateforme doit fournir des recommandations en termes de bonnes pratiques vous permettant de savoir quels contrôles activer. Cela facilitera la sécurisation de vos communications au quotidien.

RingCentral : une approche de premier plan pour une solution UCaaS de confiance

RingCentral est la référence sur le marché en matière de communications unifiées et fiables pour les entreprises qui ont adopté le numérique, et offre à chaque utilisateur des communications sûres et confidentielles. Chez nous, la sécurité est un engagement de longue date, reposant sur une expertise approfondie en matière d'exploitation et de protection des communications unifiées et des produits SaaS.

La sécurité fait partie de notre identité. Nous adoptons une approche multidimensionnelle afin de mettre la sécurité de vos données au premier rang de nos priorités, en appliquant les technologies innovantes et des processus rigoureux.

Un système de sécurité infaillible

Conçu par des experts en sécurité informatique présentant plus de 100 années d'expérience cumulées et une équipe de développement dédiée, axée sur la sécurité des données et de la plateforme.

Les meilleures pratiques DevSecOps

De la conception de nos produits jusqu'aux opérations de notre entreprise, nous employons des pratiques rigoureuses en matière de sécurité et de protection des données dans tout ce que nous faisons.
Nous offrons à nos clients une plateforme de sécurité robuste en intégrant des principes de sécurité dans le processus de développement dès le départ.

Une plateforme conçue pour être sécurisée

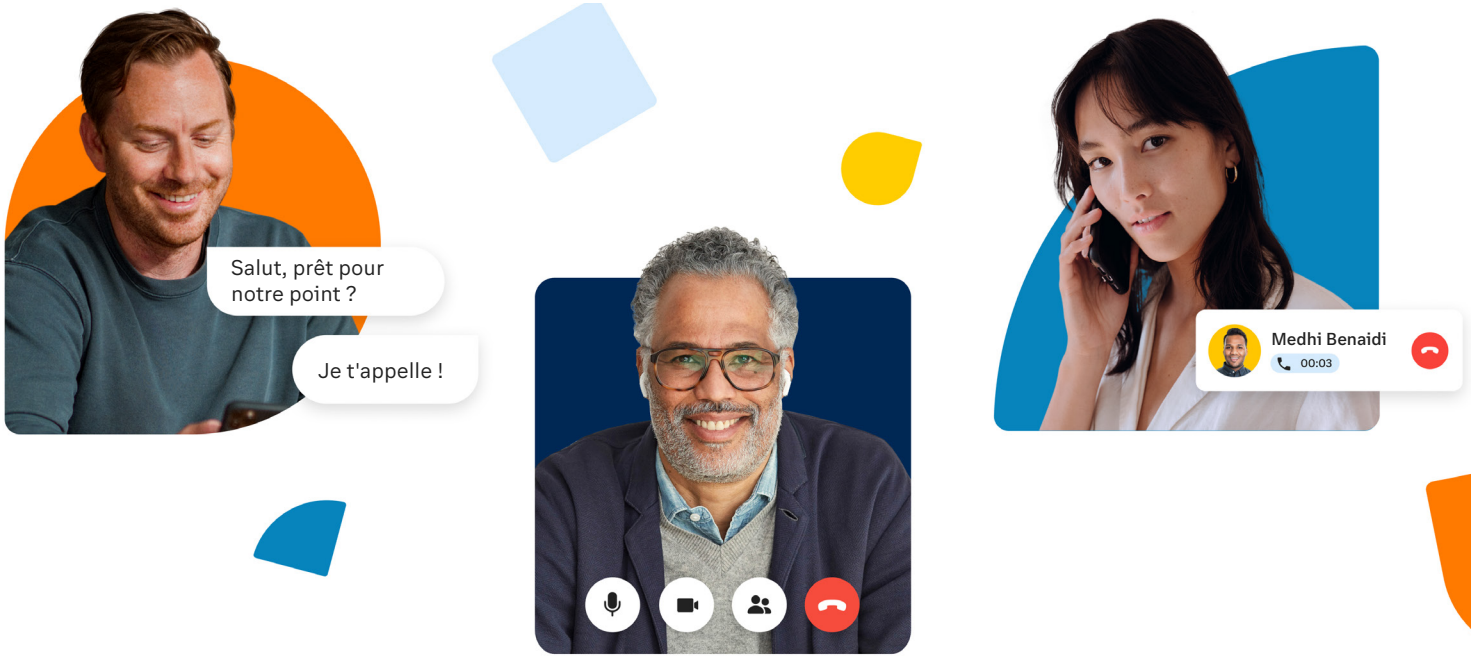
Nous nous appliquons sans relâche à maintenir un modèle de responsabilité partagée intégrant des attestations et certifications de tiers qui valident nos politiques et pratiques en matière de sécurité des informations, ainsi que des contrôles réalisés par les clients, ce qui vous permet de gérer directement vos besoins pratiques.

Un niveau de disponibilité et de fiabilité élevé

Des experts surveillent et optimisent de manière proactive notre plateforme 24h/24 et 7j/7, tout au long de l'année, afin de garantir le plus haut niveau de disponibilité de vos services.

Cet engagement se traduit par un accord de niveau de service inégalé, avec une disponibilité de 99,999 % dans plus de 45 pays. Nous maintenons ce niveau de disponibilité depuis 18 trimestres consécutifs.

Avec plus de 15 centres de données et points de présence à l'échelle planétaire, RingCentral offre une infrastructure mondiale qui garantit la continuité de vos activités 24 heures sur 24, 7 jours sur 7, partout dans le monde.



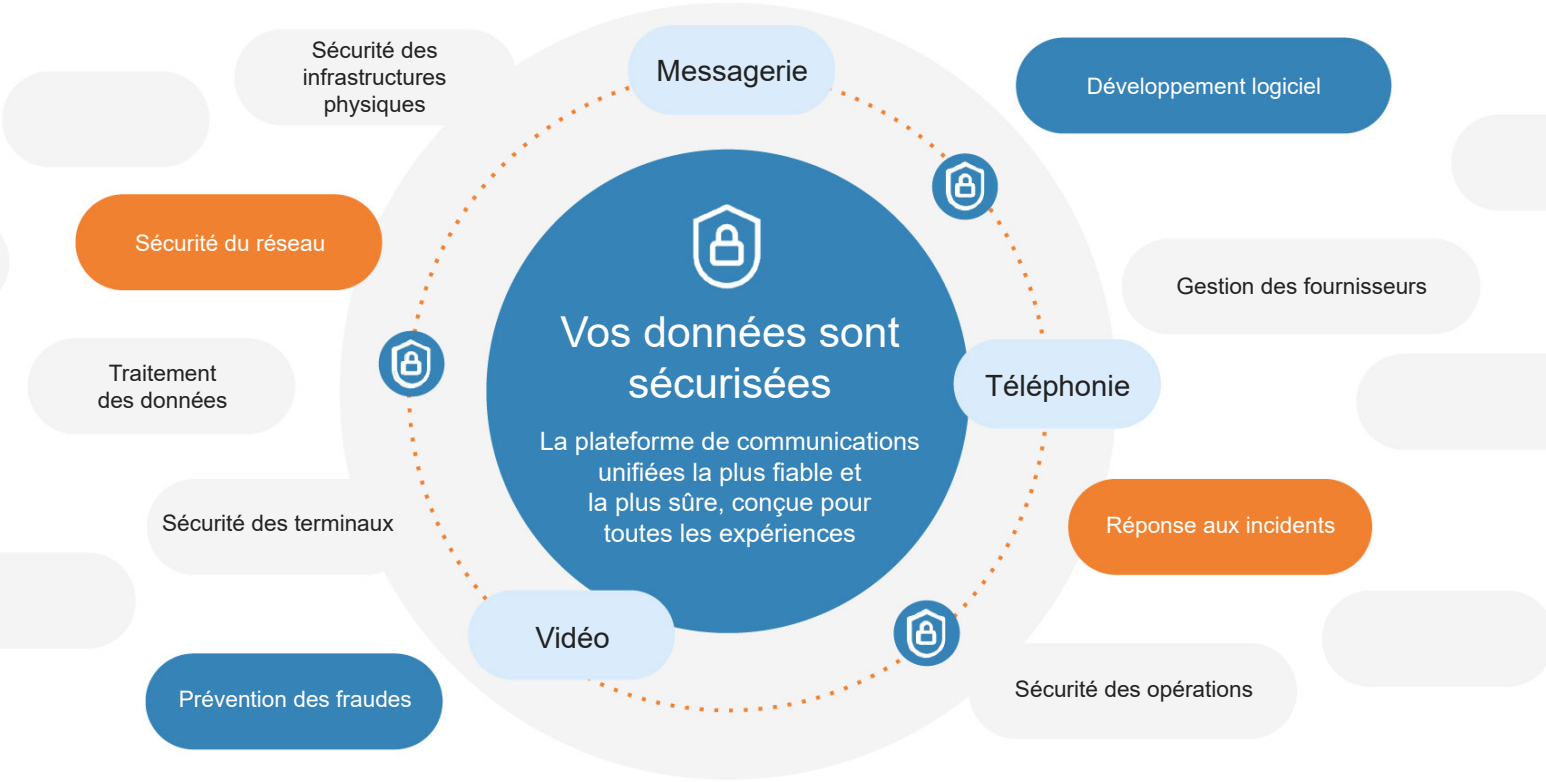
Approfondissement : protection de la sécurité des informations + gestion de la confidentialité des données et de la conformité

Actif en continu

Sécurité des informations, gestion de la confidentialité et de la conformité

Contrôles dynamiques et personnalisables en matière de sécurité et d'application des politiques

Pour vous donner une idée plus précise de nos pratiques rigoureuses, passons en revue les personnes, les processus et les technologies sur lesquels nous nous appuyons pour offrir à nos clients une expérience unique à la fois fiable, conforme et sécurisée.



1. Notre infrastructure sécurisée

L'approche de RingCentral en matière de sécurité comporte de nombreux contrôles qui reflètent les meilleures pratiques issues des normes établies du secteur en matière de sécurité informatique. Collectivement, ces contrôles rigoureux nous permettent de garantir à nos clients un niveau de sécurité de premier ordre. Parmi ces contrôles figurent :

Sécurité des infrastructures physiques

Nous mettons en place des contrôles de sécurité physique adaptés 24h/24 et 7j/7. Dans la mesure où RingCentral exploite ou utilise des centres de données (datacentres), nous veillons à ce que les contrôles de sécurité physique soient conformes aux normes du secteur, notamment ISO 27001 et SSAE 16 ou ISAE 3402.

Sécurité du réseau

Nous avons établi un programme de sécurité réseau à plusieurs niveaux, comprenant notamment : une protection par pare-feu selon les standards du secteur, des systèmes de détection des intrusions (IDS), des systèmes de prévention des intrusions (IPS), des systèmes de blocage des attaques par déni de service distribué (DDoS) et de blocage d'autres menaces venant du web, l'authentification à deux facteurs pour l'accès aux réseaux de RingCentral, et bien d'autres. Par ailleurs, nous procédons au moins une fois par trimestre à des évaluations de la vulnérabilité des réseaux internes et externes par rapport à nos systèmes de traitement des informations, afin d'apprécier régulièrement notre programme de sécurité réseau.

Chiffrement des données

RingCentral chiffre les données en transit comme au repos grâce aux standards et protocoles de chiffrement les plus innovants. Nous utilisons deux protocoles de sécurité de pointe pour garantir un niveau de sécurité supplémentaire aux appels IP : l'authentification TLS et le chiffrement SRTP.

Par ailleurs, tous les portails sont en https (par exemple, service.ringcentral.fr) ; toutes les données non vocales sont chiffrées par TLS ; et les téléphones physiques utilisent des certificats digitaux pour établir des connexions sécurisées afin de télécharger leurs données de configuration.

Pour éliminer les points faibles associés au plan de données VoIP, RingCentral protège les communications vocales à l'aide d'une technologie de pointe qui empêche l'écoute illicite d'appels ou la falsification des flux audio entre terminaux.

Prévention des fraudes

Notre équipe de gestion des abus de service et des fraudes procède à une surveillance régulière et reste à l'affût des fraudes. Nous utilisons toute une série d'outils de détection, surveillant notamment :

- Volume, rapidité, anciennes et tendances actuelles sur certaines plages, numéros composés et format de numérotation douteux
- Utilisation anormale et/ou suspecte passant par notre réseau
- Accès non autorisé à des extensions/messageries, lignes digitales, terminaux SIP et SVI

Notre équipe répond aux alertes des fournisseurs lorsqu'une activité anormale est détectée, par exemple l'utilisation de plages internationales à haut risque et à coûts élevés, le signalement d'arnaques (par ex., le numéro d'un client RingCentral a été signalé comme responsable d'arnaques, de fraudes, d'hameçonnage, etc.), ainsi que tous les signalements de harcèlement, d'appels non sollicités ou gênants.

Réponse aux incidents

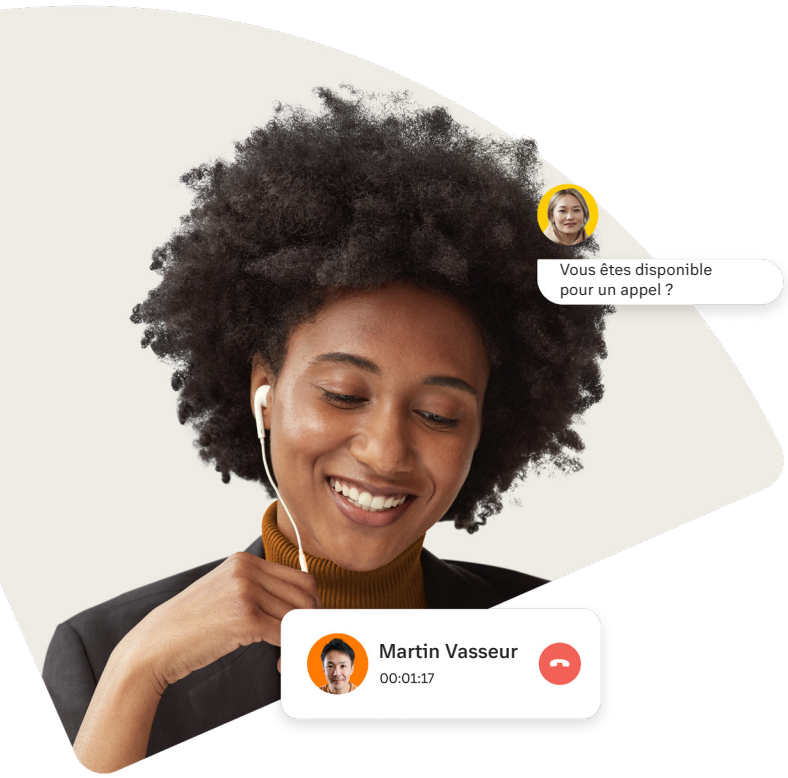
Notre faculté à réagir en cas d'incident nous permet de satisfaire aux obligations statutaires et réglementaires en la matière. Pour cela, nous maintenons un certain nombre de mesures nous permettant de réagir à tout moment aux événements susceptibles de nuire à la confidentialité, à l'intégrité ou à la disponibilité de vos services ou données, y compris des données protégées.

Données protégées

Nous avons établi un programme écrit de sécurité des informations comprenant des règles de traitement des données protégées conformes au contrat et à la législation en vigueur. Ce programme comprend par ailleurs des dispositifs de sauvegarde administratifs, techniques et physiques conçus pour préserver la confidentialité, l'intégrité et la disponibilité des données protégées.

Sécurité des opérations

Notre rigoureux programme de sécurité des opérations repose sur les meilleures pratiques du secteur et s'applique à l'ensemble de notre organisation à l'échelle mondiale. Il comprend des mesures de sécurité avancées pour la gestion des ressources, la gestion de la configuration, la protection contre les codes malveillants, la gestion des vulnérabilités et des correctifs, ainsi que la surveillance des journaux de bord.



Gestion des fournisseurs

Nous soumettons nos fournisseurs tiers aux mêmes normes de sécurité élevées et nous surveillons en permanence l'impact des vulnérabilités et expositions rendues publiques sur les produits et systèmes d'information de nos fournisseurs.

Traitement des données

RingCentral applique les normes de classification des données pour les données publiques (c'est-à-dire, les données généralement en libre accès ou que l'on peut considérer comme connues du grand public) et les données confidentielles (c'est-à-dire, les données qui ne sont pas à la disposition du grand public, notamment les données protégées).

Cycle de développement logiciel

Nous avons recours à des pratiques sécurisées en matière de cycle de développement, notamment pendant les cycles de conception, de développement et de test. Nous veillons à ce que nos produits soient soumis à des contrôles de sécurité, portant notamment sur la prise en compte des menaces et sur les pratiques de traitement des données.

2. Approfondissement : certifications et attestations en matière de protection des données et de sécurité

Les attestations et certifications que nous avons reçues de la part de tiers témoignent de notre engagement pour assurer la sécurité des données. RingCentral repose sur une plateforme cloud sécurisée affichant une large gamme de certifications en matière de sécurité et de conformité, notamment :

- Attestation SOC 2
- Attestation SOC 3
- Certifications ISO 27001 et ISO 27017-18
- STIR/SHAKEN (blocage des spams)
- Certificat HITRUST
- Attestation de conformité HIPAA
- RGPD
- Marchand certifié PCI
- PIPEDA
- C5

Cela signifie que vos données de communications (mobiles, vidéo et téléphonie) sont sécurisées, confidentielles et conformes aux réglementations en vigueur, ce qui fait de RingCentral la plateforme de communications unifiées sur le cloud la plus fiable et la plus sûre, conçue pour toutes les expériences. Vous pouvez consulter la liste complète et trouver d'autres informations sur nos certifications indépendantes ici.

3. Approfondissement : contrôles de la politique de sécurité et d'administration

La plateforme RingCentral offre à nos clients des contrôles de premier ordre en matière de sécurité et d'application des politiques, permettant à vos utilisateurs de bénéficier d'une expérience fiable et sécurisée. Notre plateforme propose tout un ensemble de contrôles administratifs pour les visioconférences, les messages et les appels téléphoniques, comme l'obligation d'authentification pour les participants à vos réunions, la définition des personnes pouvant activer le partage d'écran et l'obligation du passage en salle d'attente avant d'être autorisé à rejoindre une réunion. Vous bénéficiez ainsi des fonctions de sécurité pour protéger votre entreprise des pertes de données et des personnes mal intentionnées.

Vidéo

- Authentification unique (SSO)
- Disponible via l'application logicielle et mobile, et via un navigateur (via WebRTC)
- Mot de passe requis
- Limitation du partage d'écran
- Salles d'attente obligatoires
- Participation aux réunions réservée aux utilisateurs authentifiés
- Possibilité d'autoriser les utilisateurs à activer l'enregistrement des réunions
- Possibilité pour l'organisateur d'activer / de désactiver la vidéo pour tous les participants

- Possibilité pour l'organisateur de supprimer des participants
- Possibilité pour l'organisateur de couper le micro des participants
- Arrière-plan virtuel pour plus de confidentialité
- Possibilité de masquer l’ID de réunion
- Possibilité de contrôler le partage de fichiers de données
- Journal de bord pour suivre les modifications
- Activation du chiffrement de bout en bout (E2EE) avant la réunion
- Activation dynamique du chiffrement de bout en bout (E2EE) pendant la réunion
- Appels vocaux sécurisés avec chiffrement TLS/SRTP

Téléphone

- Authentification unique (SSO)
- Blocage de numéros de téléphone
- Blocage des spams basé sur l’IA
- Masquage du numéro
- RingOut – appels passés sur des terminaux tiers avec votre numéro de téléphone professionnel
- Routage des messages vocaux en fonction des heures d’ouverture
- Portail d'analyses
- Disponibilité de 99,999 % garantie par SLA
- Chiffrement de bout en bout des appels
- Appels vocaux sécurisés avec chiffrement TLS/SRTP

Messagerie

- Liste de contacts autorisés ou bloqués — domaines d'invités externes
- Liste de contacts autorisés ou bloqués — comptes de messagerie électronique
- Possibilité d'effacer l'identification de l'invité dans les chats entre deux interlocuteurs ou en groupe
- Possibilité d'imposer des règles
- Conforme à SEA FINRA 17a-4
- Chiffrement de bout en bout des conversations

Accès et identité

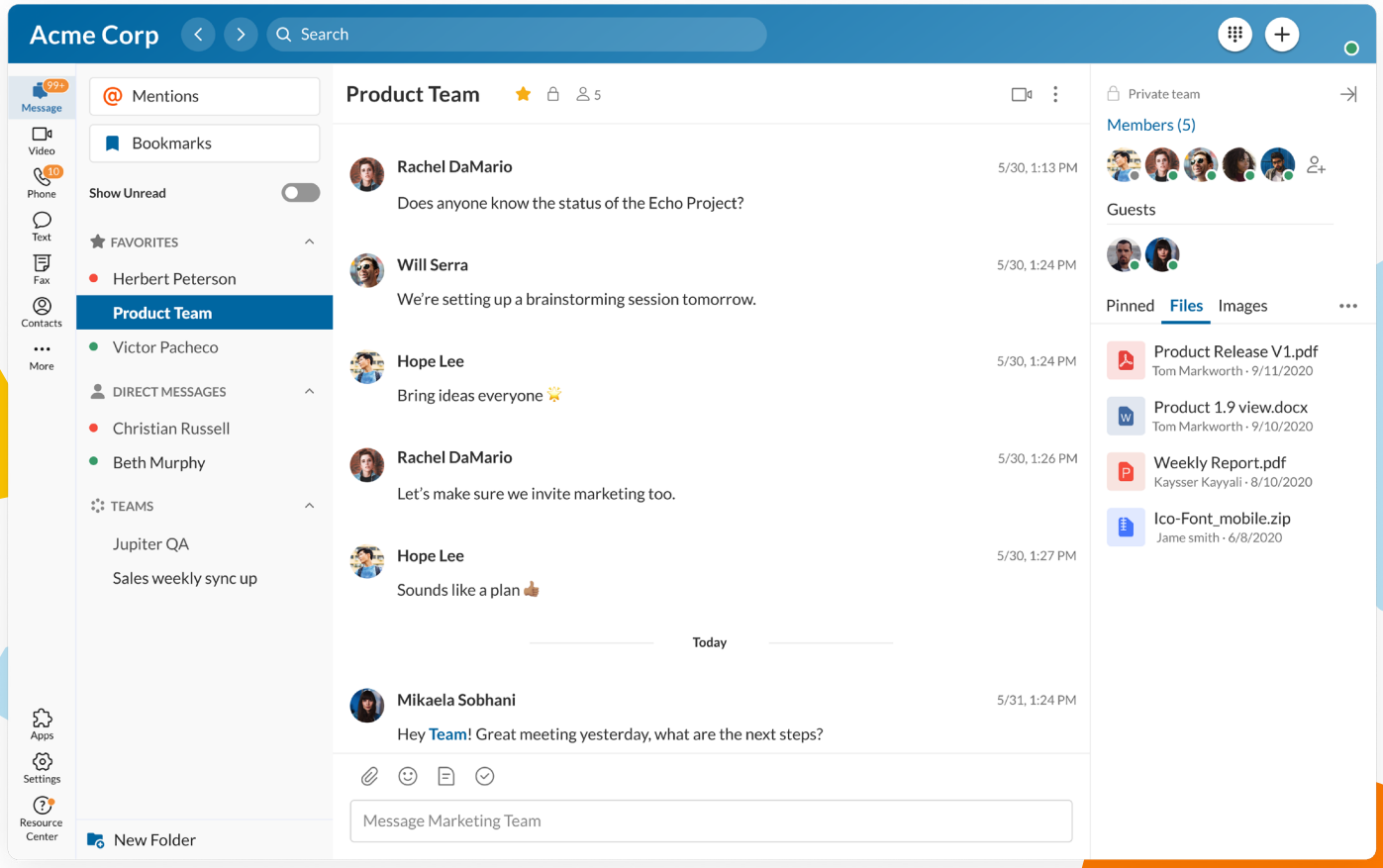
- Authentification unique (SSO)
- Authentification multifactorielle (MFA) imposée
- Application de PIN pour les terminaux
- Gestion des utilisateurs

Chiffrement

- Chiffrement des données stockées
- Chiffrement des données en transit
- Appels vocaux sécurisés avec chiffrement TLS/SRTP
- Chiffrement de bout en bout via MLS (Message Layer Security)

Application unifiée

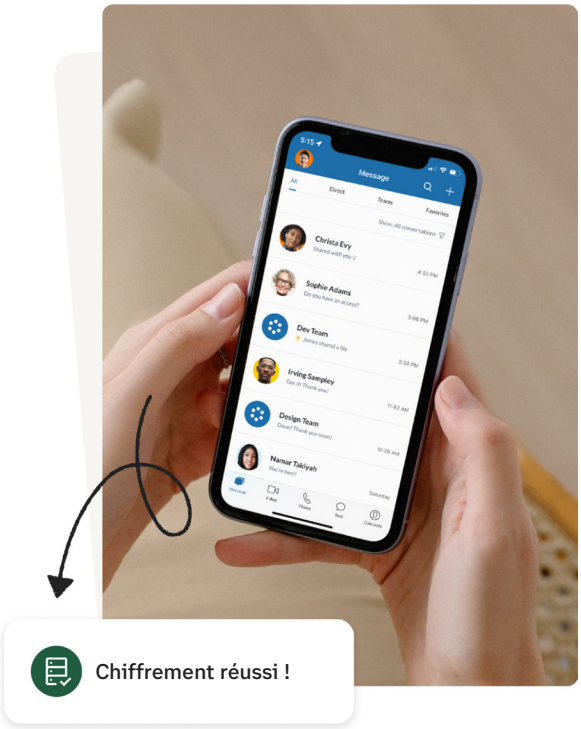
- Authentification unique (SSO)
- Disponible via l'application logicielle et mobile, et via un navigateur (via WebRTC)
- Mot de passe requis
- Accès limité aux utilisateurs authentifiés
- Minuterie de session avec déconnexion en cas d'inactivité
- Gestionnaire d'applications autorisées
- Blocage de pays pour la VoIP
- Gestion informatique centralisée des utilisateurs gratuits et payants
- Journal de bord pour suivre les modifications



Focus sur les innovations : chiffrement de bout en bout pour les appels, la messagerie et les visioconférences

Un chiffrement de première classe :

- Ne se limite pas aux appels entre deux interlocuteurs, prend en charge jusqu'à 50 participants
- Multimodal et disponible sur tous les terminaux, fixes ou mobiles
- Disponible que la conversation soit en cours, programmée ou spontanée



Avant le chiffrement de bout en bout (E2EE de l'anglais « End-to-End Encryption ») proposé par RingCentral, les utilisateurs souhaitant préserver la confidentialité de leurs appels, conversations par messages, ou visioconférences devaient s'appuyer sur plusieurs produits ne répondant pas assez bien aux normes de conformité. Ils en venaient souvent à s'affranchir des politiques d'entreprise et à utiliser des applications non validées.

Avec le chiffrement de bout en bout de RingCentral pour les appels, les messages et les réunions, aucun tiers - même pas RingCentral - ne peut accéder aux données de communication de votre entreprise. Le chiffrement de bout en bout offre des paramètres intuitifs permettant de convertir les conversations du quotidien en discussions chiffrées de bout en bout, à la fois au niveau individuel et pour les échanges en équipe.

Le chiffrement de bout en bout de RingCentral apporte une sécurité et une confidentialité inégalées pour les conversations sensibles, ainsi qu'une protection contre les intrusions de tiers et autres types d'attaques. Il supprime la nécessité de recourir à plusieurs produits de chiffrement, modernise l'expérience de l'utilisateur et réduit les problèmes de sécurité des conversations confidentielles.

Nous sommes le seul fournisseur UCaaS proposant un chiffrement de bout en bout prêt à l'emploi pour toutes les formes de communications d'entreprise, en cours, programmées ou spontanées, jusqu'à 50 participants.

Que la discussion soit en cours, programmée ou spontanée, cette couche de sécurité permet à vos utilisateurs de bénéficier du même niveau de confidentialité que celui dont ils bénéficieraient dans le cadre d'une conversation en tête à tête dans une salle de réunion.

Conformité pour les messages par chat

Les administrateurs IT de l'entreprise disposant des autorisations adéquates peuvent accéder aux données des chats dans le tableau de bord d'administration de RingCentral. Si nécessaire, ils peuvent autoriser des auditeurs tiers à accéder aux données.

RingCentral n'a pas accès aux données. Pour les organisations où la conformité est un impératif majeur, comme celles proposant des services financiers, les administrateurs peuvent désactiver le chiffrement de bout en bout au niveau de l'organisation. Pour une plus grande tranquillité d'esprit, RingCentral s'intègre étroitement avec Theta Lake pour les contrôles de conformité et les exigences de supervision sur les appels vocaux, les discussions par message et les appels vidéo avec RingCentral.

Conclusion

Les plateformes UCaaS jouent un rôle majeur dans le développement de la collaboration au sein des entreprises et par conséquent dans leur croissance. En vous associant à un fournisseur UCaaS qui donne la priorité à la sécurité, la confidentialité et la conformité en continu de vos données, vous pourrez répondre aux besoins de votre entreprise, en toute sécurité. Si vous cherchez une plateforme en tenant compte de critères qui garantissent à vos clients une expérience toujours en toute confiance, votre choix se portera naturellement sur la plateforme de RingCentral.

RingCentral offre une approche fondamentalement différente en termes de sécurité pour ce qui est de votre plateforme de communications unifiées. Avec notre taux de fiabilité de 99,999 %, inégalé sur le marché, notre système complet de protection de la sécurité de l'information et notre gestion mondiale de la confidentialité des données, vous savez que vos données sont entre de bonnes mains et vous n'avez pas à vous soucier des aspects réglementaires.

Nos innovations et notre engagement en faveur de la sécurité de la protection des données confidentielles et de la conformité nous ont permis d'être reconnus comme des pionniers sur le marché et d'être désignés leaders du Magic Quadrant de Gartner en matière de communications unifiées en tant que service (UCaaS) pendant huit années consécutives.

Notre approche assure la sécurité de l'information et la protection des données confidentielles en continu : vos données sont en sécurité et en conformité avec la législation. Notre plateforme fournit par ailleurs un ensemble complet d'outils pour vos administrateurs et utilisateurs, avec tout un éventail de contrôles dynamiques et en temps réel.

Pour en savoir plus, visitez le Centre de gestion de la confidentialité RingCentral.

Pour plus d'informations, n'hésitez pas à prendre contact avec un représentant commercial. Rendez-vous sur ringcentral.com/fr/fr/ ou composez le 0800 90 39 18.

RingCentral

857133860 02/2023

RingCentral, Inc. (NYSE: RNG) est un fournisseur leader de solutions de communications et de centre de contact dans le cloud pour les entreprises, basées sur la plateforme mondiale Message Video Phone (MVP[MD]). Plus flexible et rentable que les PBX sur site et les systèmes de visioconférences qu'elles remplacent, les solutions RingCentral permettent aux collaborateurs de communiquer en tout lieu et sur tout terminal. RingCentral propose trois produits phares dans son portefeuille. RingCentral MVP[MD] combine la messagerie d'équipe, les visioconférence, la téléphonie cloud et d'autres fonctionnalités, en une seule interface. RingCentral Video[MD], dotée aussi d'une messagerie d'équipe, permet des réunions de type Smart Video Meetings. RingCentral Centre de Contact[MD] apporte aux entreprises les outils dont ils ont besoin pour se connecter avec leurs clients sur tous les canaux. Ces produits sont disponibles sur la plateforme ouverte de RingCentral, qui intègre des centaines d'applications tierces et facilite la personnalisation de la gestion des flux. Le siège de RingCentral est situé à Belmont en Californie, et l'entreprise possède des bureaux dans le monde entier.

RingCentral France SAS, 3-5 rue Saint-Georges, 75009 Paris, France. ringcentral.com/fr/fr/

© 2023 RingCentral, Inc. Tous droits réservés. RingCentral, le logo RingCentral, et toutes les marques identifiées par les symboles [MD] ou [MC] sont des marques déposées de RingCentral, Inc. Les éventuels autres marques et logos de tiers figurant dans le présent document appartiennent à leurs propriétaires respectifs.