Ring

Chiffrement avec suppression de la clé | chiffrement de bout en bout

26 août 2026. Nous pouvons mettre à jour ce document ponctuellement afin de refléter les améliorations que nous apportons pour mieux répondre aux besoins de nos utilisateurs, notamment le renforcement des protections, l'optimisation des performances et l'amélioration de la résilience.

Résumé

La mission de Ring est de rendre les quartiers plus sûrs. La confidentialité, la sécurité et le contrôle par les utilisateurs sont au cœur de cette mission. Jusqu'à présent, Ring protégeait les vidéos de ses utilisateurs grâce à un chiffrement conforme aux normes du secteur. Par défaut, tout le contenu vidéo est chiffré durant sa transmission et son stockage dans le cloud. Ring propose également, le chiffrement de bout en bout en option, pour les utilisateurs souhaitant bénéficier d'un contrôle maximal. Ring a été le premier grand fournisseur de caméras de surveillance à domicile connectées à proposer cette fonctionnalité. Cet article présente une évolution majeure de nos solutions de chiffrement.

Sommaire

(TAKE ou Throw Away the Key Encryption) Le chiffrement avec suppression de la clé est progressivement déployé en tant que nouveau chiffrement par défaut pour tous les utilisateurs Ring. Il offre un contrôle accru sur la manière dont Ring peut traiter vos vidéos et le moment où ce traitement peut avoir lieu, tout en conservant les fonctionnalités déjà utilisées. Avec TAKE, vos vidéos sont protégées par des clés régulièrement renouvelées, et Ring ne peut déverrouiller sa copie de ces clés qu'au sein d'une enclave sécurisée. L'accès de Ring à cette enclave est limité par des contrôles d'accès, le chiffrement et l'isolation matérielle. Ring ne peut ainsi utiliser les clés que pour activer les fonctionnalités disponibles sur votre compte et supprime définitivement sa copie de vos clés après 24 heures. Si vous activez ultérieurement une fonctionnalité nécessitant le traitement de vidéos plus anciennes, votre application Ring peut fournir temporairement les clés nécessaires pour activer cette fonctionnalité. Ring les supprime ensuite à nouveau.

Le chiffrement de bout en bout (End-to-End Encryption, E2EE) reste disponible en option. Avec ce mode, Ring n'a jamais accès au contenu, même temporairement. Ring stocke uniquement les vidéos chiffrées et ne peut pas les déchiffrer : seul l'utilisateur détient les clés nécessaires pour y accéder. Les fonctionnalités nécessitant le traitement des vidéos par Ring, comme la recherche vidéo, les descriptions vidéo et les utilisateurs en partage, ne sont pas disponibles avec le chiffrement de bout en bout. Les fonctionnalités ne nécessitant aucun traitement des vidéos par Ring, comme la vidéo en direct, la lecture des événements et l'enregistrement continu, restent disponibles.

Pourquoi cela est important : Ring a conçu TAKE[1] comme son chiffrement par défaut le plus avancé à ce jour. Avec TAKE, la copie de vos clés détenue par Ring est déverrouillée au sein d'une enclave sécurisée, qui ne les libère que pour activer les fonctionnalités disponibles sur votre compte. Ring supprime définitivement cette copie après 24 heures. Vous seul en conservez une copie durable. Cette mise à niveau renforce l'un des engagements fondamentaux de Ring : intégrer la confidentialité dès la conception. Cette architecture constitue une base que nous continuerons à développer et à renforcer.

Les deux modes, TAKE et E2EE, seront disponibles pour tous les utilisateurs disposant de caméras de surveillance Ring compatibles, quel que soit leur statut d'abonnement. TAKE est déployé progressivement et les utilisateurs seront avertis lorsqu'ils pourront s'inscrire. Pour en savoir plus sur les fonctionnalités compatibles avec TAKE durant la période de déploiement, consultez **l'aide Ring**.

[1] TAKE deviendra le niveau de chiffrement par défaut de Ring une fois qu'il sera entièrement déployé auprès de l'ensemble des utilisateurs.

Cet article décrit la nouvelle architecture de chiffrement des vidéos capturées par les caméras Ring et stockées sur l'infrastructure de Ring.[1][2] Les vidéos que les utilisateurs choisissent de partager avec des tiers en dehors de Ring sont soumises aux propres dispositifs de sécurité de ces tiers.

[1] Ce livre blanc décrit comment l'architecture de chiffrement Ring protège les vidéos stockées pour le compte des utilisateurs dans le cadre d'un abonnement Ring, y compris pendant les essais gratuits. Il ne s'applique pas aux vidéos que les utilisateurs choisissent de partager avec Ring ou avec des tiers, notamment via l'outil de don de vidéos de Ring, les liens de partage ou Neighbors.

[2] Comme décrit plus en détail dans cet article, certaines méthodes de récupération et la compatibilité des fonctionnalités ne seront pas disponibles tant que TAKE n'aura pas été déployé auprès de l'ensemble des utilisateurs.

Ce que cela signifie en pratique

Avec TAKE :

1. Votre sonnette détecte les mouvements à votre porte d'entrée et vous en avertit. Vos vidéos sont protégées par des clés régulièrement renouvelées. Ring reçoit une copie de ces clés et la déverrouille au sein d'une enclave sécurisée.
2. Ring utilise temporairement ces clés pour traiter la vidéo et prendre en charge les fonctionnalités actives sur votre compte, telles que la recherche vidéo.
3. Au bout de 24 heures, Ring supprime définitivement sa copie des clés et ne peut plus traiter vos vidéos de manière autonome.
4. Une semaine plus tard, vous ouvrez l'application Ring pour regarder le clip. Ring ne disposant plus des clés, votre application lui fournit la clé nécessaire pour préparer la vidéo à la lecture, par exemple en adaptant sa qualité à votre connexion. Une fois ce traitement terminé, Ring supprime cette clé. Votre smartphone, votre tablette ou votre navigateur web déchiffre ensuite la vidéo afin que vous puissiez la regarder.

Avec le chiffrement de bout en bout :

1. Votre sonnette détecte les mouvements sur le pas de votre porte d'entrée et vous en avertit. Vos vidéos sont chiffrées avec des clés régulièrement renouvelées. Ring ne reçoit pas de copie de ces clés.
2. Ring stocke la vidéo chiffrée et la diffuse sur vos appareils, mais ne peut pas la déchiffrer.
3. Ring ne possède pas les clés, il n'y a donc rien à supprimer pour Ring.
4. Une semaine plus tard, vous ouvrez l'application Ring pour regarder le clip. Aucune clé n'est envoyée à Ring, qui ne peut donc pas préparer la vidéo à la lecture. Votre smartphone, votre tablette ou votre navigateur web déchiffre et lit directement la vidéo.
5. Étant seul à détenir les clés, les fonctionnalités telles que la recherche vidéo, les descriptions vidéo et les utilisateurs en partage ne sont pas disponibles.

TAKE vous donne un accès complet aux fonctionnalités tout en renforçant vos contrôles. Les utilisateurs qui privilégient un contrôle exclusif sans accès aux fonctionnalités cloud peuvent activer le chiffrement de bout en bout. Les vidéos restent protégées selon le mode utilisé lors de leur enregistrement, même si vous changez de mode par la suite. Ce changement s'applique uniquement aux nouveaux enregistrements.

Ce qui change avec la fonctionnalité TAKE

TAKE deviendra le nouveau mode de chiffrement par défaut pour les vidéos Ring. Une fois entièrement déployé auprès de l'ensemble des utilisateurs, il remplacera le mode de chiffrement par défaut actuel. Il s'appuie sur les protections existantes de Ring et apporte plusieurs changements importants :

	AUJOURD'HUI	AVEC TAKE
CHIFFREMENT PAR DEFAUT	Le contenu vidéo est chiffré durant la transmission et le stockage	Toutes les protections existantes, renforcées par un niveau de chiffrement propre à chaque caméra, avec des clés uniques régulièrement et automatiquement renouvelées.
ACCES AU CLOUD	Les services cloud Ring peuvent accéder à la vidéo	Les services cloud Ring peuvent accéder aux clés uniquement pour activer les fonctionnalités disponibles sur votre compte et pendant une période maximale de 24 heures. Passé ce délai, Ring ne peut accéder à une clé que si votre application Ring la lui fournit pour activer une fonctionnalité que vous utilisez.
SUPPRESSION DE CLE	Aucune suppression	Ring supprime les clés toutes les 24 heures. Une fois supprimées, ces clés ne sont plus conservées.
VOS SMARTPHONES, TABLETTES ET NAVIGATEURS WEB	Vous pouvez visionner vos vidéos	Vos smartphones, tablettes et navigateurs Web conservent leurs propres clés, pour que vous puissiez visionner vos vidéos à tout moment, même après que Ring en ait supprimé une copie.

Récupération des clés

TAKE et E2EE proposent plusieurs méthodes de récupération permettant aux utilisateurs de conserver l'accès à leurs vidéos en cas de perte de leur appareil. Ring ne peut toutefois pas procéder à la récupération à leur place. Les utilisateurs peuvent choisir parmi plusieurs méthodes de récupération, qui seront toutes disponibles une fois TAKE entièrement déployé. Si vous êtes inscrit à TAKE, vous pouvez consulter les méthodes de récupération disponibles dans l'application Ring en accédant à Centre de contrôle > Chiffrement vidéo > Caméras inscrites.

MODE DE RECUPERATION	COMMENT ÇA MARCHE	TAKE	E2EE
SAUVEGARDE DANS LE CLOUD (IOS)	Votre clé est stockée dans le trousseau iCloud et restaurée automatiquement sur votre nouvel iPhone ou iPad.	Oui	Oui
SAUVEGARDE DANS LE CLOUD (ANDROID)	Votre clé est stockée dans Google Blockstore et Google Drive, et restaurée sur votre nouveau téléphone ou tablette Android.	Oui	Oui

NOTIFICATION PUSH/CODE QR	L'un de vos smartphones ou tablettes existants approuve le nouveau	Oui	Oui
PHRASE DE CHIFFREMENT	Vous saisissez votre phrase de chiffrement de récupération sur le nouveau smartphone ou la nouvelle tablette	Oui	Oui
RECUPERATION PAR CAMERA	Votre clé est stockée sur votre caméra Ring. Ouvrez l'application Ring sur votre nouveau téléphone et approchez-vous de votre caméra Ring. L'application se connecte via Bluetooth ou wifi pour rétablir l'accès. Cette méthode est activée par défaut sur les caméras dotées d'un matériel compatible. Vous pouvez la désactiver si vous ne souhaitez pas stocker de clés sur vos caméras Ring.	Oui	Non.
CLE D'ACCES	Vous vous connectez avec une clé d'accès incluant un accès chiffré à vos clés	Oui	Oui

La récupération est conçue pour être automatique dans la mesure du possible. Si une récupération manuelle est nécessaire, la phrase de récupération générée lors de l'inscription fonctionne sur tous les appareils et toutes les plateformes, offrant ainsi une solution de secours universelle.

Partage de vidéos et accès sous TAKE

Seuls les smartphones, tablettes et navigateurs web inscrits peuvent visionner les vidéos déchiffrées. Si vous supprimez un smartphone ou une tablette de votre compte, cet appareil n'aura plus accès à vos vidéos. Le partage de l'accès aux caméras avec les utilisateurs en partage fonctionne de la même manière : lorsque vous donnez à une personne accès à l'une de vos caméras, ses appareils peuvent visionner les vidéos déchiffrées de cette caméra. Les personnes que vous ajoutez ne peuvent pas visionner les enregistrements réalisés avant leur ajout. Vous pouvez supprimer leur accès à tout moment et, une fois celui-ci supprimé, elles ne peuvent plus accéder à vos vidéos.

Vous décidez si, quand et avec qui vous souhaitez partager vos vidéos. Vous pouvez partager des enregistrements directement depuis l'application Ring avec vos proches ou toute autre personne de votre choix. Vous pouvez également télécharger des vidéos afin de les partager par d'autres moyens. Dans les régions où la fonctionnalité Demandes de la communauté de Ring est disponible, vous pouvez choisir de partager les enregistrements pertinents avec une agence locale de sécurité publique afin de contribuer à une enquête officielle dans votre région. Nous avons également mis à jour nos Directives relatives aux forces de l'ordre afin de refléter les changements liés à l'architecture TAKE.