Ring

Verschlüsselung mit anschließender Schlüsselvernichtung | Ende-zu-Ende-Verschlüsselung

26. August 2026. Wir aktualisieren dieses Dokument von Zeit zu Zeit, um die Verbesserungen abzubilden, mit denen wir unsere Kunden begeistern möchten, wie z. B. stärkere Schutzmaßnahmen, eine optimierte Leistung oder höhere Ausfallsicherheit.

Überblick

Die Mission von Ring ist es, dir die Möglichkeit zu geben, immer alles im Blick und unter Kontrolle zu behalten. Datenschutz, Sicherheit und Selbstbestimmung der Kunden stehen dabei im Mittelpunkt. Bisher hat Ring die Videos seiner Kunden mit branchenüblicher Verschlüsselung geschützt. Standardmäßig werden alle Videoinhalte von Kunden bei der Übertragung und Speicherung in der Cloud verschlüsselt. Als erster großer Anbieter von Smart Security für zuhause bietet Ring optional eine Ende-zu-Ende-Verschlüsselung für Kunden an, die maximale Kontrolle wünschen. Dieses Dokument beschreibt eine bedeutende Weiterentwicklung der Verschlüsselung von Ring.

Zusammenfassung

Die Verschlüsselung mit anschließender Schlüsselvernichtung (TAKE) wird schrittweise als neue Standardverschlüsselung für alle Ring-Kunden eingeführt. Damit hast du noch mehr Kontrolle darüber, wie und wann Ring deine Videos verarbeiten kann, während die Funktionen, die du bereits nutzt, erhalten bleiben. Mit TAKE werden deine Videos mit Schlüsseln verschlüsselt, die sich regelmäßig ändern. Ring kann seine Kopie dieser Schlüssel ausschließlich innerhalb einer sicheren Enklave entschlüsseln. Der Zugang von Ring zu dieser Enklave ist durch Zugriffskontrollen, kryptografische Verfahren und Hardware-Isolierung beschränkt. So kann Ring die Schlüssel nur für die Funktionen verwenden, die in deinem Konto aktiv sind. Nach 24 Stunden löscht Ring seine Kopie deiner Schlüssel dauerhaft. Wenn du später eine Funktion aktivierst, die ältere Videos verarbeiten muss, kann deine Ring-App vorübergehend die Schlüssel bereitstellen, um diese Funktion zu unterstützen. Anschließend löscht Ring sie erneut.

Die Ende-zu-Ende-Verschlüsselung (E2EE) steht dir weiterhin als Option zur Verfügung. In diesem optionalen Modus hat Ring keinen Zugriff auf Inhalte – auch nicht vorübergehend. Ring speichert ausschließlich verschlüsselte Videos und kann sie nicht entschlüsseln. Nur du hast die Schlüssel, mit denen sich deine Videos entschlüsseln lassen. Funktionen, für die Ring Videos verarbeiten muss (z. B. die Videosuche, Videobeschreibung und gemeinsame Nutzer), stehen mit E2EE nicht zur Verfügung. Funktionen, die keine Verarbeitung durch Ring erfordern (z. B. Live-Video, Ereigniswiedergabe und 24/7-Aufnahme), funktionieren weiterhin.

Warum das wichtig ist: Ring hat TAKE als bislang stärkste [1]Standardverschlüsselung entwickelt. Mit TAKE wird die Kopie deiner Schlüssel bei Ring innerhalb einer sicheren Enklave entschlüsselt. Die Enklave gibt sie ausschließlich für die Funktionen frei, die in deinem Konto aktiv sind. Nach 24 Stunden löscht Ring diese Kopie dauerhaft und nur du behältst eine dauerhafte Kopie. Diese Weiterentwicklung bekräftigt ein Versprechen: Datenschutz ist ein Grundprinzip dafür, wie wir bei Ring entwickeln und gestalten. Diese Architektur stellt die Grundlage dar, in die wir weiter investieren und die wir weiter stärken werden.

Beide Modi (TAKE und E2EE) stehen allen Nutzern mit unterstützten Ring-Kameras unabhängig vom Abonnementstatus zur Verfügung. TAKE wird schrittweise eingeführt und wir benachrichtigen dich, sobald du es aktivieren kannst. Weitere Informationen dazu, welche Funktionen während der Einführungsphase mit TAKE kompatibel sind, findest du im **Ring Help Center**.

[1] TAKE wird zur Standardverschlüsselung von Ring, sobald sie vollständig für alle Kunden aktiviert wurde.

Dieses Dokument beschreibt die neue Verschlüsselungsarchitektur von Ring für Videos, die mit Ring-Kameras aufgezeichnet und auf der Infrastruktur von Ring gespeichert werden.[1,2] Für Videos, die Kunden mit Dritten außerhalb von Ring teilen, gelten die Sicherheitsstandards dieser Dritten.

[1] Dieses Whitepaper beschreibt, wie die Verschlüsselungsarchitektur von Ring Videos schützt, die im Rahmen eines Ring-Abonnements (einschließlich kostenloser Testphasen) für Kunden gespeichert werden. Es gilt nicht für Videos, die Kunden mit Ring oder anderen teilen, z. B. Videos, die über das Videospenden-Tool von Ring, Freigabelinks oder Nachbarn geteilt werden.
[2] Wie in diesem Dokument näher beschrieben, stehen bestimmte Wiederherstellungsmethoden und Funktionskompatibilitäten erst zur Verfügung, wenn TAKE für alle Kunden eingeführt wurde.

Was dies in der Praxis bedeutet

Mit TAKE:

1. Deine Türklingel erfasst eine Bewegung vor deiner Haustür und benachrichtigt dich. Deine Videos werden mit Schlüsseln verschlüsselt, die sich regelmäßig ändern. Ring erhält eine Kopie dieser Schlüssel und entschlüsselt sie in einer sicheren Enklave.
2. Ring nutzt diese Schlüssel temporär, um das Video zu verarbeiten und damit Funktionen zu unterstützen, die in deinem Konto aktiv sind, wie z. B. die Videosuche.
3. Nach 24 Stunden löscht Ring die Kopie der Schlüssel dauerhaft und kann deine Videos nicht mehr eigenständig verarbeiten.
4. Eine Woche später öffnest du die Ring-App, um den Clip anzusehen. Da Ring die Schlüssel nicht mehr gespeichert hat, stellt deine App den Schlüssel zur Verfügung, den Ring benötigt, um das Video für die Wiedergabe vorzubereiten sowie z. B. die Videoqualität an deine Internetverbindung anzupassen. Ring löscht diesen Schlüssel, sobald die Verarbeitung abgeschlossen ist. Dein Smartphone, Tablet oder Webbrowser entschlüsselt anschließend das Video, damit du es ansehen kannst.

Mit Ende-zu-Ende-Verschlüsselung:

1. Deine Türklingel erfasst eine Bewegung vor deiner Haustür und benachrichtigt dich. Deine Videos werden mit Schlüsseln verschlüsselt, die sich regelmäßig ändern. Ring erhält keine Kopie dieser Schlüssel.
2. Ring speichert das verschlüsselte Video und sendet es an deine Geräte, kann es jedoch zu keinem Zeitpunkt entschlüsseln.
3. Ring hat die Schlüssel zu keiner Zeit, daher gibt es für Ring nichts zu löschen.
4. Eine Woche später öffnest du die Ring-App, um den Clip anzusehen. Es wird kein Schlüssel an Ring gesendet, daher kann Ring das Video nicht für die Wiedergabe vorbereiten. Dein Smartphone, Tablet oder Webbrowser entschlüsselt es und gibt es eigenständig wieder.
5. Da nur du die Schlüssel hast, stehen Funktionen wie die Videosuche, Videobeschreibungen oder gemeinsame Nutzer nicht zur Verfügung.

TAKE bietet dir vollen Zugriff auf alle Funktionen bei stärkeren Kontrollmöglichkeiten. Wer die alleinige Kontrolle bevorzugt und keine Cloud-Funktionen benötigt, kann die Ende-zu-Ende-Verschlüsselung aktivieren. Videos bleiben durch den Modus geschützt, in dem sie aufgezeichnet wurden, auch wenn du später den Modus wechselst. Ein Moduswechsel wirkt sich nur auf neue Aufzeichnungen aus.

Was sich mit TAKE ändert

TAKE wird zum neuen Standard für Ring-Videos und ersetzt den bisherigen Standard, sobald die Einführung für alle Kunden abgeschlossen ist. TAKE baut auf den bestehenden Schutzmaßnahmen von Ring auf und ergänzt sie um mehrere wesentliche Neuerungen:

	HEUTE	MIT TAKE
STANDARDVERSCHLÜSSELUNG	Videoinhalte werden bei der Übertragung und Speicherung verschlüsselt	Alle bisherigen Schutzmaßnahmen bleiben erhalten. Zusätzlich fügt jede Kamera eine eigene Verschlüsselungsebene mit einzigartigen Schlüsseln hinzu, die sich regelmäßig und automatisch ändern.
CLOUD-ZUGRIFF	Die Cloud-Dienste von Ring können auf Videos zugreifen	Die Cloud-Dienste von Ring können nur auf Schlüssel für aktive Funktionen in deinem Konto zugreifen, und nur während des 24-Stunden-Zeitfensters. Danach kann Ring nur noch auf einen Schlüssel zugreifen, wenn die Ring-App ihn für eine von dir genutzte Funktion bereitstellt.
LÖSCHEN DES SCHLÜSSELS	Keine Löschung	Ring löscht Schlüssel alle 24 Stunden. Nach dem Löschen speichert Ring diese Schlüssel nicht mehr.
DEINE SMARTPHONES, TABLETS UND WEBBROWSER	Du kannst deine Videos ansehen	Das Gleiche. Deine Smartphones, Tablets und Webbrowser behalten ihre eigenen Schlüssel, sodass du deine Videos jederzeit ansehen kannst, auch wenn Ring die Kopie gelöscht hat.

Schlüsselwiederherstellung

TAKE und E2EE bieten mehrere Wiederherstellungsmethoden, damit Kunden auch bei Verlust eines Geräts weiterhin auf ihre Videos zugreifen können. Ring kann diese Schritte nicht für den Kunden ausführen. Die Wiederherstellung erfolgt eigenständig: Der Kunde wählt aus mehreren Methoden, wobei alle Methoden zur Verfügung stehen, sobald die Einführung von TAKE abgeschlossen ist. Wenn TAKE für dich aktiv ist, kannst du in der Ring-App unter Control Center > Videoverschlüsselung > Registrierte Kameras prüfen, welche Wiederherstellungsmethoden verfügbar sind.

WIEDERHERSTELLUNGSMETHODE	SO FUNKTIONIERT'S	TAKE	E2EE
CLOUD-BACKUP (IOS)	Dein Schlüssel wird im iCloud-Schlüsselbund gespeichert und automatisch auf einem neuen iPhone oder iPad wiederhergestellt	Ja	Ja
CLOUD-BACKUP (ANDROID)	Dein Schlüssel wird im Google Blockstore und in Google Drive gespeichert und auf einem neuen Android-Smartphone oder -Tablet wiederhergestellt	Ja	Ja
PUSH-BENACHRICHTIGUNG / QR-CODE	Eines deiner vorhandenen Smartphones oder Tablets genehmigt das neue	Ja	Ja

PASSPHRASE	Du gibst deine Passphrase für die Wiederherstellung auf dem neuen Smartphone oder Tablet ein	Ja	Ja
KAMERABASIERTE WIEDERHERSTELLUNG	Dein Schlüssel wird auf deiner Ring-Kamera gespeichert. Du öffnest die Ring-App auf einem neuen Smartphone, hältst dich in der Nähe deiner Ring-Kamera auf, und die App stellt über Bluetooth oder WLAN eine Verbindung her, um den Zugriff wiederherzustellen. Bei TAKE für Kameras mit kompatibler Hardware standardmäßig aktiviert. Kann deaktiviert werden, wenn du keine Schlüssel auf deinen Ring-Kameras speichern möchtest.	Ja	Nein
PASSKEY	Du meldest dich mit einem Passkey an, der verschlüsselten Zugriff auf deine Schlüssel enthält	Ja	Ja

Die Wiederherstellung soll nach Möglichkeit automatisch erfolgen. Wer sie manuell durchführen muss, kann die Passphrase verwenden, die bei der Aktivierung erzeugt wurde. Sie funktioniert auf jedem Gerät und jeder Plattform und ist damit die universelle Rückfalloption.

Videos und Zugriff mit TAKE teilen

Nur registrierte Smartphones, Tablets und Webbrowser können entschlüsselte Videos anzeigen. Wenn du ein Smartphone oder Tablet aus deinem Konto entfernst, hat es keinen Zugriff mehr auf deine Videos. Für die Freigabe an gemeinsame Nutzer gilt dasselbe: Wenn du einer anderen Person Zugriff auf eine deiner Kameras gewährst, können ihre Geräte entschlüsselte Videos dieser Kamera anzeigen. Aufnahmen, die vor der Freigabe entstanden sind, kann diese Person nicht ansehen. Du kannst den Zugriff jederzeit wieder entziehen. Danach hat sie keinen Zugriff mehr auf deine Videos.

Du entscheidest, ob, wann und mit wem du deine Videos teilst. Du kannst Aufnahmen direkt aus der Ring-App mit Freunden, Familie oder anderen Personen deiner Wahl teilen, und du kannst Videos herunterladen, um sie auf anderem Weg weiterzugeben. In Regionen, in denen die Funktion „Community Request" von Ring verfügbar ist, kannst du relevante Aufnahmen mit einer örtlichen Sicherheitsbehörde teilen, um eine offizielle Ermittlung in deiner Umgebung zu unterstützen. Außerdem haben wir unsere Richtlinien für Strafverfolgungsbehörden an die Änderungen angepasst, die sich aus der TAKE-Architektur ergeben.