



Crittografia con distruzione della chiave | Crittografia end-to-end

26 agosto 2026. Potremmo aggiornare questo documento di tanto in tanto per riflettere i miglioramenti che apportiamo per soddisfare i clienti, come il rafforzamento delle protezioni, l'ottimizzazione delle prestazioni e l'aumento della resilienza.

Riassunto

La missione di Ring è rendere i quartieri più sicuri. Privacy, sicurezza e controllo da parte dei clienti sono fondamentali per raggiungere tale obiettivo. Fino ad oggi, Ring ha protetto i video dei clienti utilizzando la crittografia standard del settore. Per impostazione predefinita, tutti i contenuti video dei clienti sono crittografati durante il trasferimento e l'archiviazione nel cloud. Ring offre anche la crittografia end-to-end come opzione per i clienti che desiderano avere il massimo controllo, diventando così il primo grande fornitore di videocamere di sicurezza domestica intelligenti a offrire questa funzione. Questo documento descrive un aggiornamento significativo alle offerte di crittografia di Ring.

Riepilogo

La crittografia con distruzione della chiave (TAKE) sarà gradualmente implementata come nuova crittografia predefinita per tutti i clienti Ring. Questa tecnologia ti offre un controllo ancora maggiore su come e quando Ring può elaborare i tuoi video, mantenendo al contempo le funzionalità che già utilizzi. Con TAKE, i video vengono crittografati con chiavi che cambiano frequentemente e Ring può aprire la sua copia di tali chiavi solo all'interno di un'enclave sicura. L'accesso di Ring all'enclave è limitato da controlli di accesso, crittografia e isolamento hardware, in modo che Ring possa utilizzare le chiavi solo per attivare le funzioni attive sul tuo account. Ring elimina definitivamente la copia delle tue chiavi dopo 24 ore. Se in seguito attivi una funzione che deve elaborare video meno recenti, l'app Ring può fornirti temporaneamente le chiavi per alimentare tale funzione e le elimina nuovamente in seguito.

La crittografia end-to-end rimane disponibile come opzione. In questa modalità, Ring non ha accesso ai contenuti, nemmeno temporaneamente. Ring memorizza esclusivamente video crittografati e non è in grado di decifrarli; solo l'utente è in possesso delle chiavi necessarie per decrittografare i video. Le funzionalità che richiedono l'elaborazione dei video da parte di Ring, come la ricerca video, la descrizione video e gli utenti condivisi, non sono disponibili con la crittografia end-to-end. Le funzionalità che non necessitano dell'elaborazione video da parte di Ring, come la visualizzazione in diretta, la riproduzione di eventi e la registrazione continua, continuano a funzionare.

Perché è importante: Ring ha progettato TAKE come modalità di crittografia predefinita¹ più potente fino ad oggi. Con TAKE, le chiavi di Ring vengono sbloccate all'interno di un ambiente sicuro e rilasciate solo per attivare le funzionalità sul tuo account. Ring elimina definitivamente la copia dopo 24 ore; solo tu ne conservi una copia permanente. Questo aggiornamento rafforza il nostro impegno a garantire la privacy, un principio fondamentale nel modo in cui progettiamo e costruiamo i nostri prodotti. Questa architettura rappresenta una base su cui continueremo a investire e a migliorare.

Entrambe le modalità (TAKE e crittografia end-to-end) saranno disponibili per tutti i clienti che fanno uso delle videocamere Ring supportate, indipendentemente dall'abbonamento. TAKE verrà implementata gradualmente e i clienti riceveranno una notifica quando potranno registrarsi. Per ulteriori informazioni sulle funzionalità compatibili con TAKE durante il periodo di implementazione, visita la pagina [Assistenza Ring](#).

¹ TAKE diventerà il livello di crittografia predefinito di Ring una volta implementato per tutti i clienti.

42 Questo documento descrive la nuova architettura di crittografia video di Ring per i video acquisiti dalle videocamere Ring e archiviati
43 nell'infrastruttura Ring.^{1,2} I video che i clienti scelgono di condividere con terze parti al di fuori di Ring sono coperti dai framework di
44 sicurezza delle terze parti stesse.
45

¹ Questo white paper descrive in che modo l'architettura di crittografia di Ring protegge i video archiviati per conto dei clienti in combinazione con un abbonamento Ring (incluso il periodo di prova gratuita). L'architettura di crittografia non si applica ai video che i clienti scelgono di condividere con Ring o terzi, ad esempio i video condivisi tramite lo strumento per la donazione di video di Ring, i link di condivisione o Neighbors.

² Come descritto più avanti in questo documento, alcuni metodi di ripristino e la compatibilità delle funzionalità non saranno disponibili fino a quando TAKE non sarà stata implementata per tutti i clienti.

Cosa significa in pratica

Con TAKE:

1. Il videocitofono rileva i movimenti alla porta d'ingresso e ti invia una notifica. I tuoi video sono crittografati con chiavi che cambiano frequentemente. Ring riceve una copia delle chiavi e le apre in un enclave sicuro.
2. Ring utilizza temporaneamente tali chiavi per elaborare il video e supportare le funzionalità attive sul tuo account, come la ricerca video.
3. Dopo 24 ore, Ring elimina definitivamente la copia delle chiavi e non può più elaborare i tuoi video.
4. Una settimana dopo, apri l'app Ring per guardare il filmato. Poiché Ring non detiene più le chiavi, l'app fornisce la chiave necessaria a Ring per preparare il video per la riproduzione, ad esempio per adattarne la qualità alla connessione. Ring elimina la chiave al termine dell'elaborazione e il telefono, il tablet o il browser web decrittografa il video per consentirti di guardarlo.

Con la crittografia end-to-end:

1. Il videocitofono rileva i movimenti alla porta d'ingresso e ti invia una notifica. I tuoi video sono crittografati con chiavi che cambiano frequentemente. Ring non riceve una copia di tali chiavi.
2. Ring archivia il video crittografato e lo invia ai tuoi dispositivi, ma non è in grado di decifrarlo in nessun momento.
3. Ring non conserva le chiavi, quindi non c'è nulla che Ring possa eliminare.
4. Una settimana dopo, apri l'app Ring per guardare il filmato. Non viene inviata alcuna chiave a Ring, quindi Ring non può preparare il video per la riproduzione; il tuo telefono, tablet o browser web lo decifra e riproduce autonomamente.
5. Poiché solo tu hai le chiavi, funzionalità come ricerca video, descrizione video e utenti condivisi non sono disponibili.

TAKE ti offre l'accesso completo alle funzionalità con controlli più potenti. I clienti che preferiscono il controllo esclusivo senza accesso alle funzionalità cloud possono attivare la crittografia end-to-end. I video rimangono protetti nella modalità in cui sono stati registrati, anche se cambi modalità in un secondo momento. La modifica delle modalità influisce solo sulle nuove registrazioni.

Cosa cambia con TAKE

TAKE sarà la nuova impostazione predefinita per i video Ring e sostituirà l'impostazione predefinita attuale una volta implementata completamente per tutti i clienti. Si basa sulle protezioni esistenti di Ring e aggiunge diverse importanti modifiche:

	OGGI	CON TAKE
CRITTOGRAFIA PREDEFINITA	Il contenuto video è crittografato in transito e a riposo	Tutte le protezioni esistenti, in più ogni videocamera aggiunge il proprio ulteriore livello di crittografia con chiavi univoche che cambiano regolarmente e automaticamente.
ACCESSO AL CLOUD	I servizi cloud di Ring possono accedere ai video	I servizi cloud Ring possono accedere alle chiavi solo per le funzionalità attive sul tuo account e solo durante la finestra di 24 ore. In seguito, Ring può accedere a una chiave solo se l'app Ring la fornisce per una funzionalità che utilizzi.
ELIMINAZIONE DELLA CHIAVE	Nessuna eliminazione	Ring elimina le chiavi ogni 24 ore. Dopo l'eliminazione, Ring non conserva più tali chiavi.
I TUOI TELEFONI, TABLET E BROWSER WEB	Puoi visualizzare i tuoi video	I tuoi telefoni, tablet e browser Web conservano le proprie chiavi, così puoi visualizzare i tuoi video in qualsiasi momento, anche dopo che Ring ne ha eliminato la copia.

Recupero della chiave

TAKE ed E2EE mettono a disposizione dei clienti diversi metodi di recupero, così che possano mantenere l'accesso ai propri video in caso di smarrimento di un dispositivo. Ring non può eseguire queste operazioni per conto del cliente. Il ripristino è self-service: una volta che TAKE è completamente implementato, il cliente può scegliere tra più metodi di ripristino. Se sei registrato a TAKE, puoi verificare i metodi di recupero disponibili nell'app Ring, accedendo a Centro di controllo > Crittografia video > Videocamere registrate.

METODO	DI	COME FUNZIONA	TAKE	E2EE
RIPRISTINO				
BACKUP SU CLOUD (IOS)		La chiave viene memorizzata nel portachiavi iCloud e viene ripristinata automaticamente sul tuo nuovo iPhone o iPad	Sì	Sì
BACKUP SU CLOUD (ANDROID)		La chiave viene archiviata in Google Blockstore e Google Drive e ripristinata sul tuo nuovo telefono o tablet Android	Sì	Sì
NOTIFICA PUSH/CODICE QR		Uno dei tuoi telefoni o tablet esistenti approva quello nuovo	Sì	Sì
PASSPHRASE		Inserisci la frase segreta di recupero sul nuovo telefono o tablet	Sì	Sì
RIPRISTINO TRAMITE VIDEOCAMERA		La chiave è memorizzata nella videocamera Ring. Apri l'app Ring su un nuovo telefono, avvicina il telefono alla videocamera e l'app si conatterà tramite Bluetooth o Wi-Fi per ripristinare l'accesso. Questa funzione è attivata per impostazione predefinita per TAKE sulle videocamere con hardware compatibile. Puoi disattivarla se non vuoi memorizzare le chiavi sulle videocamere Ring.	Sì	No

CODICE D'ACCESSO

Accedi con un codice d'accesso che include l'accesso crittografato alle tue chiavi

Sì

Sì

Il ripristino è progettato per essere automatico quando possibile. Per i clienti che devono eseguire il ripristino manualmente, la frase segreta generata durante la registrazione funziona su qualsiasi dispositivo e piattaforma, rendendola un metodo di riserva universale.

Condivisione di video e accesso alla sezione TAKE

I video decrittografati possono essere visualizzati solo dai telefoni, dai tablet e dai browser Web registrati. Se rimuovi un telefono o un tablet dal tuo account, non avrà più accesso ai tuoi video. Lo stesso principio si applica alla condivisione dell'accesso alle videocamere con altri utenti: quando concedi a una persona l'accesso a una delle tue videocamere, i suoi dispositivi possono visualizzare i video decrittografati di quella videocamera. Le persone che aggiungi non possono visualizzare le registrazioni acquisite prima dell'aggiunta e puoi rimuovere il loro accesso in qualsiasi momento; una volta rimosse, non potranno più accedere ai tuoi video.

Sei tu a decidere quando, con chi e se condividere i tuoi video. Puoi condividere le registrazioni direttamente dall'app Ring con amici, familiari o chiunque tu voglia e puoi anche scaricarle per condividerle con altri metodi. Nelle regioni in cui è disponibile la funzione Richieste di comunità di Ring, puoi scegliere di condividere le registrazioni pertinenti con un ente locale di pubblica sicurezza per sostenere un'indagine ufficiale nella tua zona. Abbiamo anche aggiornato le nostre [Linee guida per le forze dell'ordine](#) per tenere conto delle modifiche derivanti dall'architettura TAKE.
