



Throw Away the Key Encryption | End-to-End Encryption

August 26, 2026. We may update this paper from time to time to reflect the improvements we make to delight customers, such as strengthening protections, optimizing performance, and increasing resilience.

Abstract

Ring's mission is to make neighborhoods safer. Privacy, security, and customer control are foundational to that mission. Until now, Ring has protected customer videos using industry-standard encryption. By default, all customer video content is encrypted in transit and at rest in the cloud. Ring also offers End-to-End Encryption as an opt-in for customers who want maximum control, the first major provider of smart home security cameras to do so. This paper describes a significant upgrade to Ring's encryption offerings.

Summary

TAKE (Throw Away the Key Encryption) is rolling out gradually as the new default encryption for all Ring customers. It gives you even greater control over how and when Ring can process your videos, while keeping the features you already use. With TAKE, your videos are encrypted with keys that change frequently; Ring can only unlock its copy of those keys within a secure enclave. Ring's access to the enclave is restricted by access controls, cryptography, and hardware isolation, so that Ring can only use keys to power the features active on your account. Ring permanently deletes its copy of your keys after 24 hours. If you later enable a feature that needs to process older videos, your Ring app can temporarily provide the keys to power that feature, and Ring deletes them again afterward.

End-to-End Encryption (E2EE) continues to be available to customers as an option. In this optional mode, Ring does not have access to content, even temporarily. Ring stores only encrypted video and cannot decrypt it; only you hold the keys needed to decrypt video. Features that require Ring to process video, such as Video Search, Video Description, and Shared Users, are not available under E2EE. Features that do not require Ring to process video, such as Live View, event playback, and 24/7 recording, keep working.

Why this matters: Ring designed TAKE to be our strongest default¹ encryption to date. With TAKE, Ring's copy of your keys is unlocked inside a secure enclave, which releases them only to power the features active on your account, and Ring permanently deletes that copy after 24 hours; only you keep a lasting copy. This upgrade reinforces a commitment: privacy is a core principle of how we build and design at Ring. This architecture is a foundation that we will continue to invest in and strengthen.

Both modes (TAKE and E2EE) will be available to all supported Ring camera customers regardless of subscription status. TAKE is rolling out gradually, and customers will be notified when they're eligible to enroll. To learn more about which features are compatible with TAKE during the rollout period, visit [Ring Help](#).

This paper outlines Ring's new encryption architecture for video captured by Ring cameras and stored on Ring's infrastructure.^{2,3} Videos that customers choose to share with third parties outside of Ring are covered by those third-parties' own security frameworks.

¹ TAKE will become Ring's default level of encryption once it is fully rolled out to all customers.

² This whitepaper describes how Ring's encryption architecture protects videos stored on behalf of customers in connection with a Ring subscription (including free trials). It does not apply to videos customers choose to share with Ring or others, such as videos shared through Ring's video donation tool, share links, or Neighbors.

³ As described further in this paper, certain recovery methods and feature compatibility will not be available until TAKE has been rolled out to all customers.

37 **What This Means in Practice**

38 **With TAKE:**

- 39 1. Your doorbell detects motion at your front door and notifies you. Your videos are encrypted with keys that change frequently.
- 40 Ring receives a copy of those keys and unlocks them in a secure enclave.
- 41 2. Ring temporarily uses those keys to process the video to support features active on your account, such as Video Search.
- 42 3. After 24 hours, Ring permanently deletes its copy of the keys and can no longer process your videos on its own.
- 43 4. A week later, you open the Ring app to watch the clip. Because Ring no longer holds the keys, your app provides the key Ring
- 44 needs to prepare the video for playback, such as adapting the video quality to your connection. Ring deletes that key when that
- 45 processing finishes, and your phone, tablet, or web browser decrypts the video so you can watch it.

46 **With End-to-End Encryption:**

- 47 1. Your doorbell detects motion at your front door and notifies you. Your videos are encrypted with keys that change frequently.
- 48 Ring does not receive a copy of those keys.
- 49 2. Ring stores the encrypted video and delivers it to your devices, but cannot decrypt it at any point.
- 50 3. Ring doesn't hold the keys, so there is nothing for Ring to delete.
- 51 4. A week later, you open the Ring app to watch the clip. No key is sent to Ring, so Ring cannot prepare the video for playback;
- 52 your phone, tablet, or web browser decrypts and plays it on its own.
- 53 5. Because only you have the keys, features like Video Search, Video Description, and Shared Users, are not available.

54

55 TAKE gives you full feature access with stronger controls. Customers who prefer sole control with no cloud feature access, may enable

56 E2EE. Videos remain protected under the mode they were recorded in, even if you later change modes. Changing modes only affects

57 new recordings.

58 **What Changes with TAKE**

59 TAKE will be the new default for Ring videos, replacing the current default once fully rolled out to all customers. It builds on Ring's

60 existing protections and adds several important changes:

	TODAY	WITH TAKE
DEFAULT ENCRYPTION	Video Content is encrypted in transit and at rest	All existing protections, plus each camera adds its own extra layer of encryption with unique keys that change regularly and automatically.
CLOUD ACCESS	Ring's cloud services can access video	Ring cloud services can only access keys to power features active on your account, and only during the 24-hour window. After that, Ring can access a key only if your Ring app provides it for a feature you use.
KEY DELETION	No deletion	Ring deletes keys on a rolling 24-hour basis. After deletion, Ring no longer retains those keys.
YOUR PHONES, TABLETS, AND WEB BROWSERS	You can view your videos	Same. Your phones, tablets, and web browsers keep their own keys, so you can view your videos at any time, even after Ring deletes its copy.

61

62 **Key Recovery**

63 TAKE and E2EE offer several recovery methods so that customers maintain access to their videos in the event of a lost device; Ring

64 cannot perform these actions on the customer's behalf. Recovery is self-service: the customer chooses from multiple recovery methods,

65 with all methods available once TAKE is fully rolled out. If you are enrolled in TAKE, you can check which recovery methods are available

66 in the Ring App by going to Control Center > Video Encryption > Enrolled Cameras.

67

RECOVERY METHOD	HOW IT WORKS	TAKE	E2EE
CLOUD BACKUP (IOS)	Your key is stored in iCloud Keychain, restored automatically on your new iPhone or iPad	Yes	Yes
CLOUD BACKUP (ANDROID)	Your key is stored in Google Blockstore and Google Drive, and restored on your new Android phone or tablet	Yes	Yes
PUSH NOTIFICATION / QR CODE	One of your existing phone or tablet approves the new one	Yes	Yes
PASSPHRASE	You enter your recovery passphrase on the new phone or tablet	Yes	Yes
CAMERA-BASED RECOVERY	Your key is stored on your Ring camera. You open the Ring app on a new phone, stand near your Ring camera, and the app connects over Bluetooth or WiFi to restore access. On by default for TAKE for cameras with compatible hardware. Can be disabled if you do not want to store keys on your Ring cameras.	Yes	No
PASSKEY	You sign in with a passkey that includes encrypted access to your keys	Yes	Yes

69 Recovery is designed to be automatic whenever possible. For customers who need to recover manually, the passphrase generated during
70 enrollment works on any device and any platform, making it the universal fallback.
71

72 Sharing Videos and Access under TAKE

73

74 Only enrolled phones, tablets, and web browsers can view decrypted videos. If you remove a phone or tablet from your account, it no
75 longer has access to your videos. Sharing access to cameras with Shared Users works the same way: when you give another person
76 access to one of your cameras, their devices can view decrypted videos from that camera. People you add cannot view recordings
77 captured before they were added, and you can remove their access at any time; once removed, they no longer have access to your
78 videos.

79 You decide if, when, and with whom to share your videos. You can share recordings directly from the Ring app with friends, family, or
80 others you choose, and you can also download videos to share through other methods. In regions where Ring's Community Requests
81 feature is available, you can choose to share relevant recordings with a local public safety agency to support an official investigation in
82 your area. We have also updated our [Law Enforcement Guidelines](#) to reflect changes resulting from the TAKE architecture.
83
