Verkada

Enterprise Controlled Encryption (ECE)

Overview

Verkada encrypts video data at rest (i.e., on the user's device or on Verkada's cloud servers) and in transit (i.e., as data moves among devices and the cloud). ECE builds on this encryption framework by giving customers more control over their data encryption. Leveraging a well-recognized technique called client-side encryption, customers can choose to keep some keys to themselves, share them with Verkada if they need technical support, or with a third party for a variety of reasons, as outlined below. ECE improves on Verkada's already robust data protection measures–empowering customers with control over their data.

Customers must opt-in and enable ECE for their devices. ECE will not be enabled for customers by default. To opt-in, navigate to "Privacy & Security" under "Admin" settings. Click on "Enterprise Controlled Encryption" and complete all the steps.

An Added Layer of Protection	With ECE, decryption requires access to two keys: one key is on Verkada servers, while the other is stored with the customer's identity provider (e.g., Okta, Microsoft Entra ID, etc.) Both keys are required to decrypt certain data including most video history, so even if there is a breach at the identity provider or Verkada, the customer's data remains secure. ECE is, in short, an enhanced, robust security method for data storage and transfer, combining the existing secure decryption step on Verkada's servers with a second step on the customer's own devices.
Customers Control Key Access	ECE puts decryption keys directly in our customers' hands–allowing them to selectively share access on an as-needed basis. This flexibility allows customers to leverage the expertise of specialized services or comply with legal requirements, while maintaining control over their data.[1] ECE allows the customer to decide who gets access to data, for how long, and to what extent.

1. Using ECE, a customer might wish to share its decryption keys with third parties for a number of reasons. A customer can allow a cybersecurity firm to conduct a safety audit to analyze video data without having permanent device access. During a time-sensitive investigation, a customer can additionally provide specific keys to law enforcement to grant access to relevant footage without exposing their entire video archive. A customer can, moreover, use a transcoding service to change the format of video or employ translation services and grant the service provider limited, task-specific access to data.