Data Security & CJIS Compliance

Truleo follows a CJIS-compliant data transfer process where your videos stay in your evidence platform.

What is CJIS compliance?

The FBI requires criminal and noncriminal justice agencies (CJAs and NCJAs) to protect and safeguard criminal justice information (CJI), including biometric, identity history, person, organization, property and case/incident history data. The FBI's CJIS security policy provides these agencies with requirements for handling their CJI and accessing FBI CJIS systems and information. CJAs and NCJAs are ultimately responsible for ensuring compliance to this security policy, even when engaging with third-party software or services to manage or analyze CJI.

Who enforces CJIS compliance?

No central body certifies software as CJIS compliant, and so there is no official CJIS certification. Software vendors assert CJIS compliance when their software adheres to the FBI's communicated CJIS security policy.

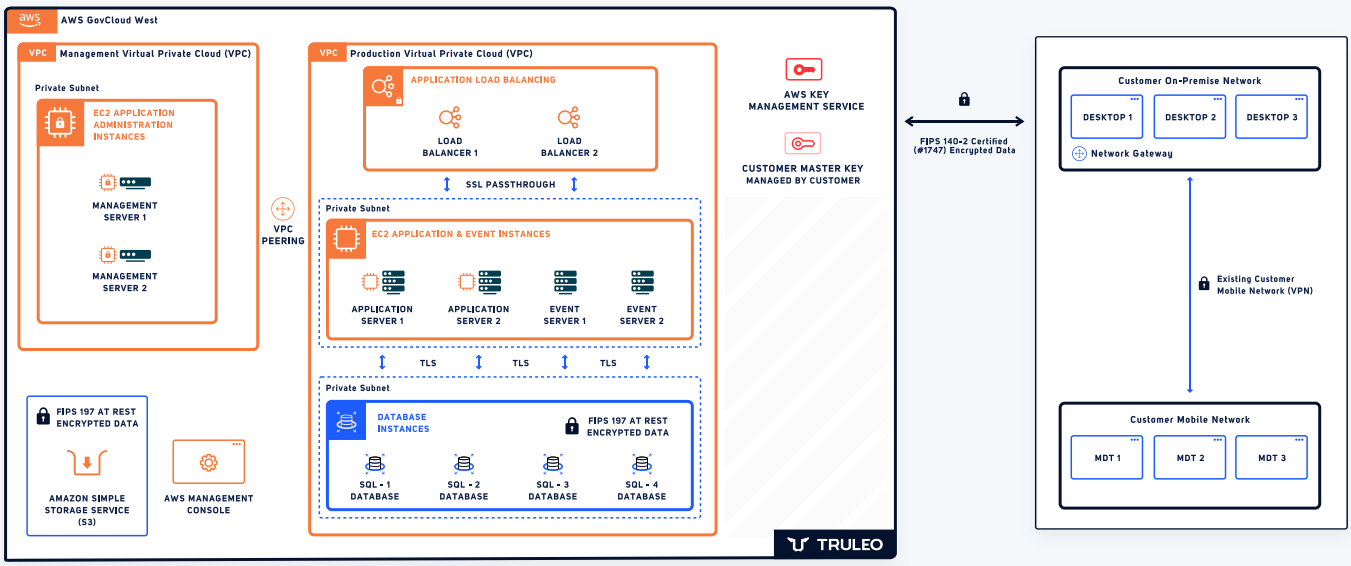
Does Truleo use CJI Data?

Truleo does not use CJI data but nevertheless maintains CJI compliance. Truleo software only analyzes the audio portion of body-worn camera footage extracted during the streaming upload process. Audio data is not directly regarded as CJI and, by itself, does not require CJIS compliance.

How does Truleo ensure CJIS compliance?

TRUSTED AND SECURE CLOUD INFRASTRUCTURE

Truleo deploys its software within AWS GovCloud, a secure cloud hosting environment that meets CJIS compliance requirements. In accordance with the CJIS security policy, AWS GovCloud ensures no unauthorized person–not even AWS personnel–have access to customer data.

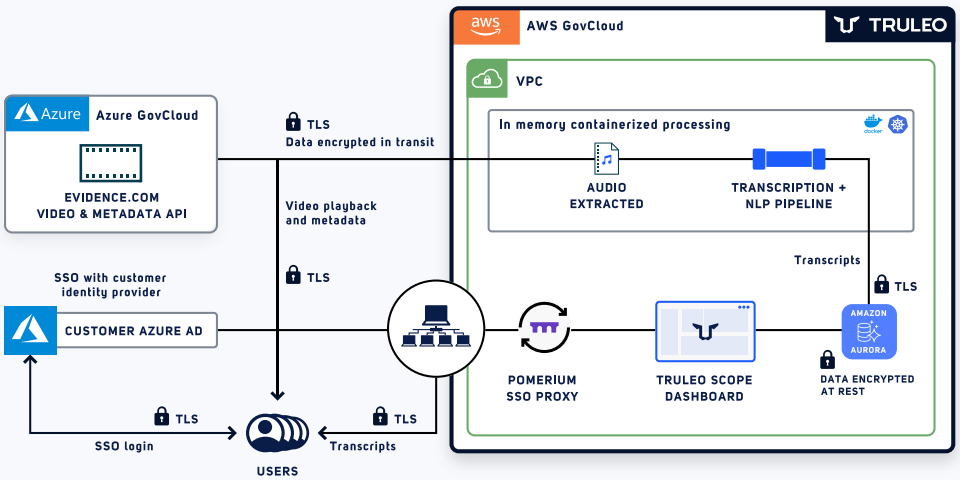


STRICT IT POLICIES

Truleo adheres to a strict set of IT security policies to ensure CJIS compliance. You can read our full set of AWS-certified security policies on our website. A few critical points of our security policies are mentioned below.

1. END-TO-END ENCRYPTION

Truleo software uses industry-standard cryptographic protocols to encrypt data both in transit (when accessing, analyzing, or moving data) and at rest (when holding data in memory or storage). Truleo's high level of data encryption means customer data is always secure.



2. SECURE DATA ACCESS

To access data through Truleo software, users must be authorized. Users are authenticated and access data from Truleo just as they do for their evidence management system. At an agency's request, Truleo will authenticate users via SSO and an approved identity provider (such as Microsoft Azure Active Directory).

3. VULNERABILITY MITIGATION AND MANAGEMENT

Truleo increases security and reduces vulnerabilities by separating our software into virtual containers. These containers prevent bugs and malicious code from spreading across different parts of Truleo software. Truleo uses vulnerability scanning tools to ensure these containers stay secure and any bugs and malicious code are eliminated quickly.

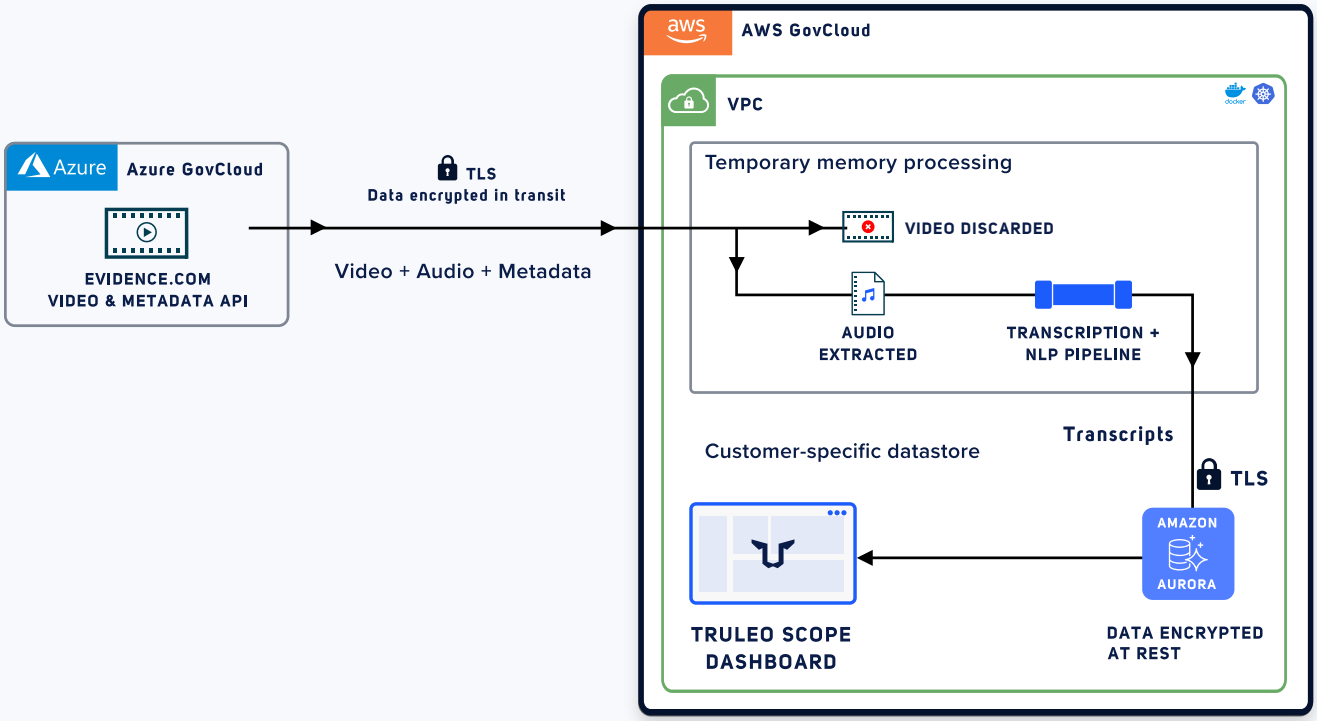
4. TRAINING AND CLEARANCE OF TRULEO PERSONNEL

All Truleo employees are trained on the CJIS security policy and Truleo's protocols for maintaining CJIS compliance. Because Truleo does not store CJI data, not all employees require background checks or other verification. Depending on the customer engagement, relevant Truleo employees undergo a customer-defined background processing (e.g., Triple-Eye) to adhere to agency policies.

5. DATA MANAGEMENT AND STORAGE

When analyzing the audio stream of a video, Truleo software does not make a copy of or store the original audio or video footage; rather, it only stores the audio transcript and analysis.

To create an audio transcript and analysis, Truleo software first requests and receives the relevant footage from an agency's evidence management system. When this footage arrives to Truleo's network, our software extracts only the audio portion of the footage and immediately discards the video, which is irrevocably wiped from the network. The audio is held in temporary memory while Truleo's machine learning models produce a transcript, labels of relevant events, and labels of professional / unprofessional language. The transcript and analysis are stored in a customer-specific data store on Truleo's network.



Once processed, the in-memory audio is discarded and no longer accessible. To reprocess the audio, Truleo software must again request it from the evidence management system. When a user requests playback of footage from the Truleo user interface, that footage comes directly from the evidence management system. Truleo does not store or copy the footage.

What is Truleo?

Truleo analyzes police body camera videos using artificial intelligence to help promote police professionalism. Truleo worked with FBI National Academy alumni to build the models that deconstruct language used during events to help agencies promote best practices, train new officers, and mitigate risk. To learn more about Truleo's mission to improve trust in the police with body camera analytics, visit www.truleo.co.

TRULEO
www.truleo.co
Truleo Inc.
1 E Erie Street ,Suite 525-2246
Chicago, IL 60611
info@truleo.co
1 (312) 219-5266