SWEAR™

SWEAR Authenticity Platform - How It Works

Blockchain-Based Authenticity for Surveillance Systems

OVERVIEW

Advances in AI are making it easier to fabricate or subtly alter surveillance footage. This is making historical methods used to protect the authenticity of digital assets for investigators and compliance teams to become outdated and obsolete. As AI media manipulation technologies accelerate, court-durable evidence demands will expand to require verifiable provenance at capture, and a continuous chain of custody across ingest, storage, and export.

This document illustrates how the SWEAR Authenticity Platform creates a new generation of AI-resistant and quantum-resistant surveillance recordings – in real time and at scale.

Certification System

The Certification System runs on video management systems (VMS) by using the vendor supplied APIs to access the video streams. As videos are written to disk by the VMS, SWEAR simultaneously creates cryptographic hashes to map every frame and second of a recording.

SWEAR does not modify any aspect of the surveillance video

Protection

SWEAR immediately preserves each cryptographic hash into an independent ledger which is protected by blockchain, creating an immutable third-party timestamp and audit trail. SWEAR maintains privacy - the blockchain ledger records only five non-identifying vectors:

- Hash value for a segment of a recording
- Time stamps for the beginning and end of a protected segment
- Time stamp when the video segment was cryptographically hashed
- Time stamp when the hash was protected in the independent ledger
- A system generated video stream ID

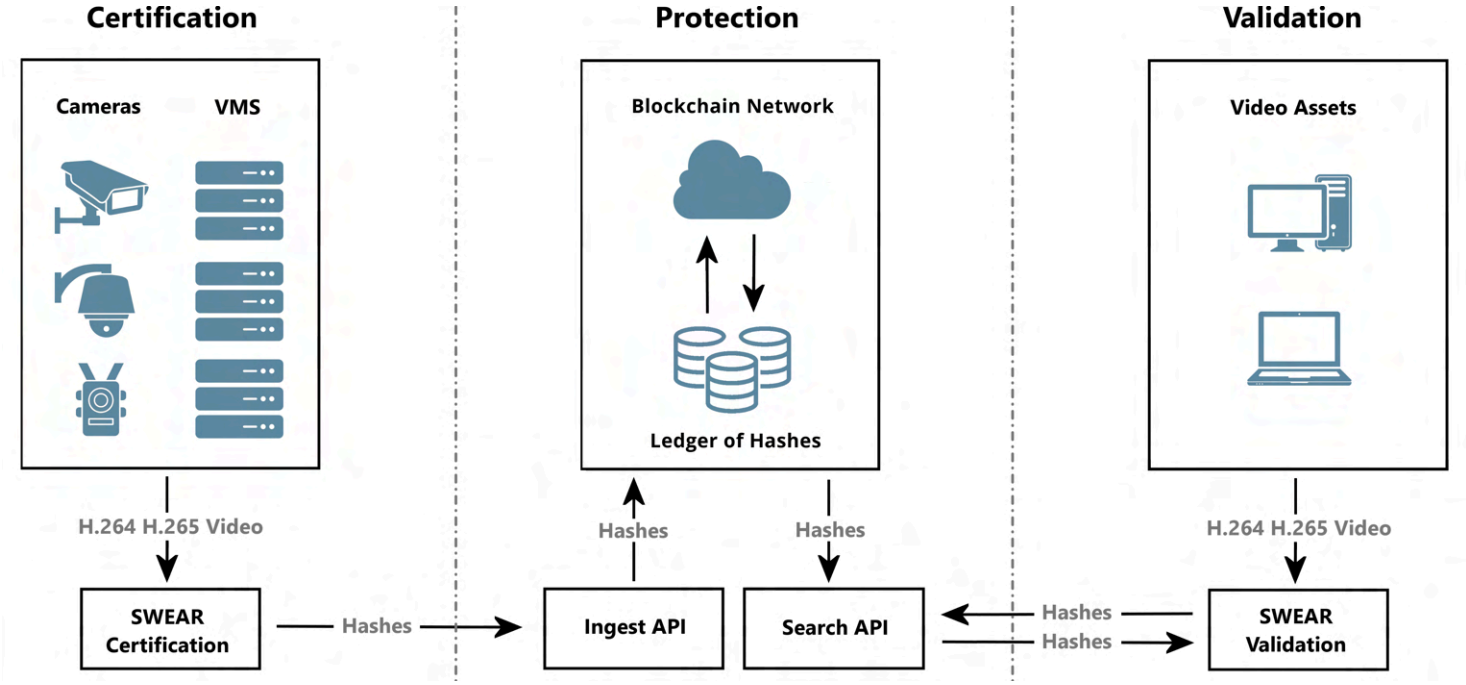
SWEAR does not collect any client information, device analytics, or media data

Validation System

When the authenticity of surveillance video footage must be validated, SWEAR re-computes cryptographic hashes for every frame and second of the submitted video and compares them to the original hashes protected by the independent blockchain network. Any mismatch—down to a single frame—flags that second as modified and inauthentic.

SWEAR can detect if a single pixel has been modified

System Architecture



Setting the Standard for Authentic Content

SWEAR defines a new global standard for digital truth. We don't chase fakes after the damage is done — we prevent tampering at its root by embedding authenticity at creation. With cryptographic fingerprints, blockchain anchoring, and real-time verification, SWEAR makes content authenticity provable, permanent, and indisputable.

For platform demonstrations, technical integration details, or partnership inquiries, please visit www.swear.com.