COMCAST TECHNOLOGY SOLUTIONS

Digital watermarking for premium VOD and high-profile sports

Crucial, real-time evidence to thwart piracy and fraud at scale

Premium video on demand (PVOD) consumption continues to grow, increasing pressure on distributors to protect high-value content. From PVOD release windows to UHD/4K assets and global live sports and entertainment events, digital watermarking has become a baseline requirement for doing business, driven by licensing agreements, brand protection, and operational risk.

At Comcast Technology Solutions (CTS), we view watermarking not as a stand-alone security feature but as a forensic accountability layer that enables faster detection, smarter response, and stronger compliance across modern over-the-top (OTT) ecosystems. Here we'll look at key watermarking approaches, architectural trade-offs, and planning considerations businesses should understand as we move through the 2020s and into the future.

Watermarking's role: Accountability at scale

Digital watermarking does not prevent piracy outright. Its value lies in what happens after content leaks. Pirates can create new accounts, but watermarking provides security teams with the hooks needed to respond quickly. Sports programming is an excellent example as a use case: Most events are over in two to three hours, but some, like a boxing match that ends in the first round, can end suddenly, putting a pay-per-view customer's value at immediate risk. Watermarking provides not only the accelerated response but also the evidence legal teams need to pursue a formal claim.

- By embedding a traceable identifier into the delivered stream or rendered output, watermarking allows leaked content to be resolved back to a specific user, session, or account.
- That forensic signal enables action: revoking access, accelerating takedowns, escalating enforcement, and limiting repeat abuse.

For premium content with high revenue or brand exposure, watermarking helps raise the cost of misuse and shortens time to action — making it a critical component of a layered content protection strategy alongside digital rights management (DRM) and credential abuse mitigation.

Client-side vs. server-side: An architectural decision

Every watermarking deployment begins with a fundamental choice: where the watermark is applied.

Client-side watermarking embeds the mark directly within the player, app, or device during playback. This enables highly dynamic payloads such as session IDs and timestamps and can reduce the exposure of unmarked content or streams.

However, it also requires deep integration and long-term maintenance across every platform and player SDK. Device diversity, update cadence, and client-side tampering all introduce operational and security complexity.

Server-side watermarking, by contrast, applies the watermark within the delivery pipeline — during transcode, packaging, at the origin, or at the content delivery network (CDN) edge. Clients remain unaware of the process, enabling faster multi-screen rollouts and a consistent user experience. This approach centralizes control and observability, and aligns naturally with DRM, logging, and large-scale live delivery.

Server-side solutions provide a more predictable path to scale and operational simplicity. Although they require additional compute and storage for watermarking variants (such as the two-step watermarking below), server-side watermarking scales easier for large libraries and large, live audiences.

Two-step (A/B) watermarking: Built for modern streaming

Most server-side deployments today rely on two-step, or A/B, watermarking:

1. Visually identical content variants typically labeled A and B are generated for each segment or subsegment. Each variant encodes different forensic information.
2. A serialization engine dynamically assembles a unique sequence of A and B segments for each viewer or session at delivery time.

This approach works seamlessly with adaptive bitrate (ABR) streaming, supports massive concurrency for live events, and keeps client applications simple. Because serialization can occur at the CDN edge, two-step watermarking scales efficiently while preserving cache performance.

Plan early for dynamic ad insertion

Dynamic ad insertion (DAI) introduces additional challenges. Ad workflows often involve separate origins and manifest manipulation, which can disrupt forensic signals if not addressed early.

- CTS helps clients ensure watermark tokens persist across manifest rewrites or are re-injected at the edge: This way, traceability survives personalized ad breaks.
- Where ad segments cannot be watermarked, graceful handling ensures playback continuity while protecting the forensic integrity of the core content.

Standards matter

Industry alignment around the European Telecommunications Standards Institute (ETSI) TS 104 002 and DASH-IF guidance has accelerated server-side A/B watermarking adoption. These standards define interoperable roles across encoders, packagers, CDNs, and detection systems — allowing CTS to integrate once and operate across vendors, platforms, and networks.

By keeping watermarking logic in the network rather than in consumer devices, CTS clients benefit from reduced tampering risk, faster launches, and lower ongoing QA overhead — while meeting the expectations of major studios and sports leagues.

A shorter, straighter line between detection and response

Watermarking is most effective when it is operationalized, well before it's deployed. At CTS, we design watermarking architectures that connect detection to response, enabling rapid revocation, enforcement, and reporting when leaks occur.

As licensing pressure increases and content value rises, the right watermarking strategy is one that fits your delivery architecture, scales with your audience, and delivers measurable results when it matters most.

How to choose

Choose client-side when:

- You control the player stack across platforms and can invest in ongoing SDK QA.
- You need highly dynamic, on-device payloads and offline scenarios.
- You're comfortable with per-device hardening strategies.

Choose server-side/two-step when:

- You want client agnosticism and a fast, multi-screen rollout.
- You prefer centralized operations, observability, and simpler UX guarantees.
- You can accommodate variant generation plus CDN edge logic.

Practical implementation at CTS

- **Client-agnostic implementation:** Works independently of client-side logic, reducing complexity for device manufacturers and app developers. CDN edge logic handles token interpretation and A/B stitching, making it cache-friendly and efficient.
- **Transcoding and packaging:** Create A/B (or more granular) variants for each representation and propagate watermark pacing and metadata downstream.
- **Cloud Video Platform (CVP):** Maintain a mapping between User_ID, Session_ID, and Watermark_ID. Orchestrate interactions between the watermarking cloud platform and the CDN to ensure secure access.
- **Rapid revocation:** Enable mechanisms to revoke access when necessary.
- **Sessioning and Tokenization:** Issue a unique watermark token per viewer (e.g., included in the path or query string) that encodes the A/B pattern for that session.
- **CDN edge logic:** Interpret the token and assemble the correct A/B sequence for each request — client-agnostic and optimized for caching.
- **DAI coexistence:** Ensure watermark tokens persist through manifest rewrites or are re-injected at the edge so watermarking remains intact during ad breaks.

CTS endorses ecosystem partnerships

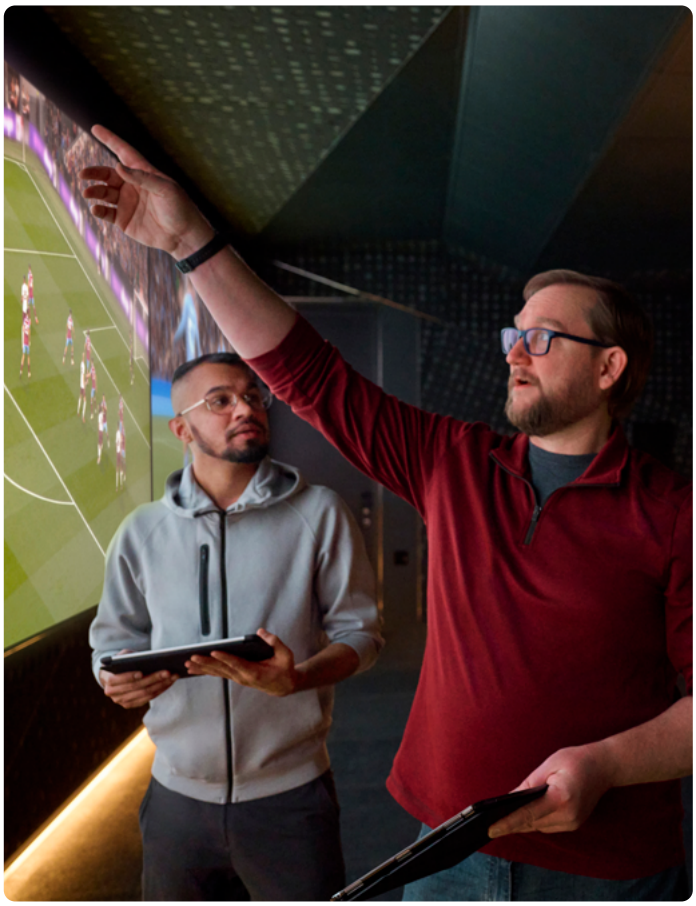
The CVP architecture is designed to support future integration with third-party, cloud-native SaaS watermarking providers (who can also offer “detection and piracy monitoring services”) aligned with ETSI standards. In the event of content leakage, the embedded watermark can be resolved to the originating account or session, enabling rapid access of revocation and supporting downstream enforcement actions.

Connect people with more of the content they love

Built on Comcast’s know-how, scalable platforms, and proven facilities and infrastructure, Comcast Technology Solutions (CTS) offers more than 30 years of reliable real-world media and advertising experience. CTS offers a powerful portfolio designed to equip media companies with the technologies, scale, and expertise to thrive and succeed in today’s rapidly evolving global media and entertainment landscape.

Find out more

www.comcasttechnologysolutions.com
comcasttechnologysolutions@comcast.com



[1] “Publicly Available Specification; DASH-IF Forensic A/B Watermarking: An operable watermaking integration schema,” ETSI, 2023

This document contains forward-looking statements regarding future products and features that are currently under development. These statements reflect our current plans and expectations, which are subject to change. We undertake no obligation to update any forward-looking statements to reflect events or circumstances after the date of this document.