Content Protection Decision Worksheet

Decide how much protection your catalog actually needs before you sign a content deal or a DRM contract. Match the layer to the threat — DRM is the heart of the stack, not the whole of it. Engineering guidance; confirm vendor numbers live, they change.

1 · NAME THE THREAT (what are you actually protecting against?)

- ☐ **Write down what one leak costs you.** 'A competitor gets our $20M original for free' is DRM territory; 'someone watches our webinar without registering' is not.
- ☐ **Classify the content:** public / low-value · private but not premium · premium or licensed · 4K or early-window.
- ☐ **Check the license.** If you license studio content, the contract specifies the protection — it is not yours to choose.

2 · MATCH THE LAYER TO THE THREAT (each stops a different attacker)

- ☐ **Access control (token auth / signed URLs)** — decides who can even ask for the manifest and segments.
- ☐ **Transport encryption (AES-128, HLS)** — scrambles the bytes; only as strong as the token auth on the key request.
- ☐ **DRM (Widevine / PlayReady / FairPlay)** — protects the KEY and the DECRYPTED BYTES in a trusted module.
- ☐ **Output protection (HDCP 2.2+) + forensic watermarking** — guard the cable; trace the leak DRM can't prevent.

3 · MAKE THE DRM CALL (don't over- or under-protect)

- ☐ **Public / low-value?** Access control may be enough — no DRM. Your call: _____
- ☐ **Private but not premium?** Token auth + AES-128 with a SECURED key server is often enough.
- ☐ **Premium or licensed?** Multi-DRM: encrypt once with cbcs, license Widevine + PlayReady + FairPlay.
- ☐ **4K or early-window?** Hardware DRM (Widevine L1 / SL3000) + HDCP 2.2 + forensic watermarking.

4 · AVOID THE FOUR CLASSIC MISTAKES

- ☐ **cenc-only encryption** silently breaks Apple — FairPlay needs cbcs. Standardize on cbcs from day one.
- ☐ **'DRM stops screen recording'** — it does not. The analog hole needs watermarking, not a 'better' DRM.
- ☐ **Open AES-128 key server** — the key sits in the manifest; without token auth the encryption is a screen door.
- ☐ **Over-protecting low-value content** while under-protecting the one title with contractual obligations.

THE ONE SANITY CHECK BEFORE YOU SIGN

Two questions decide everything. (1) What does the license require? If you are licensing content, the answer is written down and is not yours to choose — premium 4K typically mandates hardware DRM + HDCP 2.2 + forensic watermarking. (2) What does one leak actually cost? DRM is cheap relative to what it unlocks: at a representative $0.30 per 1,000 license requests, 100,000 subscribers × 50 sessions/month = 5,000,000 requests ≈ $1,500/month — about 0.125% of a $1.2M/month catalog that is only licensable with DRM in place. The real cost is the multi-DRM integration and per-device player work, not the per-license fee. Remember what DRM can't do: it protects the key and the decrypted bytes, never the camera pointed at the screen — that is what watermarking is for.