Video Protection Checklist

Kinescope

Access control decides who gets in; the rest makes the file useless if it gets out. For anything you sell, work top to bottom, then verify — free or low-stakes video may not need every layer.

1 SET ACCESS

- [ ] **Choose who can watch**
  Public, private link, password, single-use codes, or company email domain — match it to how you sell.

2 LOCK THE FILE

- [ ] **Turn on encryption at the project level**
  All videos in the project, current and future, are encrypted at once.
- [ ] **Activate both browser DRM systems**
  Widevine (Chrome, Edge, Firefox, Android) and FairPlay (Safari, iOS). One alone leaves the other half of your audience unprotected.

3 CONTROL WHERE IT PLAYS

- [ ] **Sign playback links and set them to expire**
  A link shared yesterday stops working today.
- [ ] **Restrict embedding to your own domains**
  The player refuses to load if your embed code is lifted onto another site.

4 TRACE LEAKS

- [ ] **Add a watermark on top of DRM**
  DRM already blocks screen recording on hardware-backed playback; the watermark complements it for the gaps — a desktop browser, or a camera pointed at the screen. Carrying the viewer's ID or email, it makes any leak point back to the account it came from.

5 VERIFY BEFORE YOU TRUST IT

- [ ] **Run the rip test**
  Try to download your own video. The download should fail, and anything pulled another way should refuse to play.
- [ ] **Check playback in Chrome and Safari**
  Confirm real viewers can watch on both, so DRM isn't silently breaking your Apple audience.

ON "STOP DOWNLOADS"

For the tools most people reach for, DRM blocks the download and returns an error. A determined person can still find a way to pull the encrypted pieces, but without the key the copy won't play, so there is no point.