

功能介绍

如何保障视频内容安全，防止视频被盗链、非法下载和传播，是众多企业困扰已久的问题，特别是在线教育、企业培训、财经金融等在线版权视频领域，处理不好会造成严重的经济损失或信息泄露风险。

保利威云点播提供了针对视频内容安全的多种保护机制，从产品功能、技术实现以及平台服务等多方面保障您的视频版权不受到非法侵犯。详见：[保利威PlaySafe视频版权保护体系](#)。

在技术和产品功能层面保利威提供如下的视频安全保护机制：

安全机制	描述	安全级别
播放密码	可针对视频设置播放密码，观众需输入正确的密码才能播放视频	低
视频水印	把企业专属水印编码进视频流，让视频内带有版权信息，保护公司知识产权	低
播放域名黑白名单	通过设置域名黑白名单，实现视频只能在指定网站播放的效果	较低
授权播放	视频播放前播放器调用业务方的授权验证接口，实现二次鉴权	中
录屏/抓流监测	播放器自动检测主流浏览器或手机系统的录屏/抓流行为，并警告终止播放	较高
防录屏跑马灯	将观众信息显示在视频上，并不规则地跑动，可追溯录屏者身份，对翻录行为起到强有力的警示作用。	较高
视频加密	采用私有加密算法和安全传输机制，提供云端一体的视频加密解决方案	高
安全下载	移动端（iOS/Android SDK）将加密后的视频数据缓存在本地，私钥加密存储且只有保利威播放器才可解密播放	高

播放密码

播放密码是一种简单的安全保护机制，为视频设置密码后，观众需输入正确的密码才可以播放视频。

使用方式参考：[播放密码](#)。

视频水印

水印是在视频编码时将图片压在视频流中的，水印图片成为了视频的一部分。企业可以把专属的Logo等信息作为视频水印显示在视频画面中，以此来展示企业版权信息和品牌形象。

使用方式参考：[视频水印](#)。

播放域名黑白名单

播放域名限制是在云端配置的视频资源访问策略，根据视频所在网站的域名，可配置拒绝播放视频的网站域名黑名单，或允许播放视频的网站域名白名单，以达到基本的保护目的，防止被恶意盗链播放。

使用方式参考：[播放域名设置](#)。

授权播放和防录屏跑马灯

在用户网站中，除了登录验证外，还可以通过在云点播管理后台设置授权验证接口，播放器会调用该接口去验证观众是否有播放某一个视频的权限，从而实现对观众的二次鉴权。

另外该接口还可以通过返回跑马灯的内容和样式信息，在视频播放过程中，使观众信息在视频上不规则滚动，以此来警示盗版者，达到视频版权保护的效果。

使用方式参考：[授权播放和跑马灯](#)。

录屏/抓流检测

部分浏览器（比如360浏览器）以及浏览器插件带有录屏或抓取视频流并下载的功能，保利威播放器会主动监测录屏或抓流行为，一旦发现观众开启了录屏功能或抓流插件，视频会自动停止播放并提示。保利威Android/iOS SDK也提供防录屏功能，开启防录屏开关后，在Android系统中录制的视频画面为黑色，而在iOS系统中视频会终止播放并提示。

视频加密

上述安全机制能够有效保障用户的合法访问，但对于付费观看场景，如果盗版者通过一次付费拿到视频播放URL，将视频下载到本地并进行二次分发，对于企业而言所造成的经济损失也是十分严重的。因此需要通过多种安全机制配合，共同保障视频内容安全，而其中最为重要的一项安全保护机制，就是视频加密。

保利威视频加密是对视频数据本身进行加密，加密后的视频即使被下载到本地，也是无法播放和二次分发的。视频加密可有效防止视频泄漏和盗链问题。

使用方式参考：[保利威视频加密](#)。

安全下载（离线播放）

在移动端（iOS、Android）APP，一般会有缓存、下载到本地并离线播放的业务场景，保利威移动端SDK提供的安全下载功能可以有效保护下载到本地的视频文件，防止被拷贝后恶意播放和传播。主要优点有：

1. 下载到本地的视频本身是加密的，只能通过保利威移动端SDK进行解密播放，拷贝后无法直接播放和二次分发。
2. 私钥文件加密存储，有效防止被窃取。
3. 每个视频文件都有独立的私钥，即使单个泄漏也不会影响其它视频。
4. 所有的下载、解密、播放逻辑在SDK内部实现，用户无需额外处理，简单易集成。

使用方式参考：

- [iOS SDK](#)
- [Android SDK](#)