The Ultimate Guide to Secure Video Hosting

DaCast

Introduction to Secure Hosting and Delivery for Online Video

The video streaming market is predicted to be worth $70.5 billion within two years. With that success comes an increase in privacy concerns. In today's digital world, video security represents an important challenge for many businesses and organizations. Security firms are measuring an increase in piracy and other forms of digital attack every single year.

So the logical question becomes: how can you protect your online video content?

This eBook will answer that question by examining 7 key tools to access secure video hosting in the modern world. In addition, we'll discuss how to gain reliable access to these tools and include them in your digital publishing workflow.

Industries that need secure video hosting:

- Media & OTT
- Publishing
- E-learning
- Entertainment
- Government & Institutions
- Enterprise

There are countless reasons to protect your online video. The biggest, of course, is simply that online video is valuable.

More than 4.6 million people watch music festivals via live stream each year—and the majority of these viewers are paying customers. By 2024, it's predicted that 310 million households will subscribe to at least one OTT streaming solution. An annual survey on higher education found that 88 percent of universities agree that video increases student achievement levels. Beyond these use-cases, many businesses and organizations rely on over-the-top video content for sharing sensitive information. For example, medical and educational institutions are responsible for protecting privacy and ensuring that only authorized individuals gain access to such content. If secure content leaks to the public or to competitors, businesses that use video for internal communications can experience embarrassment and outright harm. And OTT companies or people monetizing online video courses rely on maintaining control of their material.

One of the most important decisions you'll make when you publish your videos is exactly where, and by whom, you want your videos to be viewed. In many cases, distributing video entails a trade-off between accessibility and security.

For example, maybe you want to attract as big an audience as possible. In that case, you'll want to turn off all your security settings! The more people who watch, the better. On the other hand, perhaps it's vital that only a few specific people see your content. In this case, you should lock down every possible security option. For the majority of business, however, security requirements fall somewhere between these two extremes.

This eBook provides you with a go-to-guide to work through your options toward the end of deciding which security solutions are right for you. With that said, let's dive into the details. Here are our 7 methods to improve your video security via the tools that a secure streaming solution can provide.

1 Securing Your Video Stream In-Transit with Encrypted Video Delivery

Digital TV Research estimates that by 2022, piracy will cost businesses $52 billion a year. And that figure only reflects the direct cost of piracy. There exists both commercial and reputational risk in internal information that is stolen or publicly distributed by pirates.

One of the best ways to protect yourself against this sort of attack is by using encrypted video delivery. The standard encryption method is called Advanced Encryption Standard, or AES.

As the name suggests, AES adds an encryption layer to your videos. This tool makes it impossible for anyone to watch your videos unless they have a legitimate access token to decrypt the content. Anyone attempting to intercept the video between the server and the final destination will only receive junk data. If anyone tries to download the content without the encryption key, the video content simply won't play.

However, secure video streaming platforms don't widely include AES. If you want to host your video with a minimum of advanced security and you have a limited budget, AES encryption is a good place to start. When combined with other security options, this tool can greatly improve the privacy and security of your online video.

2 Choosing Your Audience with Password Protection

One simple yet often overlooked security tool is password protection. This feature allows users to set a password for a given video or live stream. Anyone who enters the correct password can gain access. Others will be blocked from viewing the stream.

Password protection is ideal for sharing videos among a relatively small group. It works best when it's also in the viewer's interest to keep the video private. This is because the viewer can always share the password with unauthorized users. That said, for quickly sharing videos with colleagues or clients for approval, or other similar use-cases, password protection is ideal.

Most of the professional online video platforms include some form of password protection. However, some OVPs do not include this feature at the first plan level, but rather only on more expensive plans. Therefore, make sure you review the level of features available in detail when selecting your OVP and plan.

3 Payment Security for Online Video Monetization

Akamai, one of the largest CDN (content delivery network) in the world, has found that credential theft for online video subscriptions is a major issue. Millions of accounts are compromised every year. And for obvious reasons, you never want to be known as the business that had a breach and exposed user credentials and payment data.

That's why payment security is so important. Any subscription or transactional video monetization program absolutely needs to be protected using SSL encryption. SSL is the same protection method used when you log in to your bank account. It's also the standard for online payments, and it's extremely secure.

To secure all payments for your online video, you need to be absolutely sure that your video paywall uses SSL encryption. The easiest way to ensure this is to use a professional video monetization platform, such as Cleeng or InPlayer. Alternatively, you can choose a video streaming platform that guarantees a secure paywall.

4 Securing Your Embedded Videos with Domain and IP Controls

Domain restriction is a security feature that allows you to explicitly specify on which domains the video will and won't play. If somebody inspects the source of your pages and tries to view or share the video link to an unauthorized website, it simply won't work. The video player will show a DCP error rather than your video content. This feature is very easy to set up.

One potential downside of any video embed is that pirates and other ill-meaning people will copy your embed code and embed your streaming video on websites that you haven't approved. It's relatively easy for somebody to copy your video embed code and them simply use it on their own website.

All it takes is a right-click on your page, a scroll through the page source, and a quick copy-paste job.

Of course, you can't stop someone from copying code. However, thanks to this feature that most professional online video platforms provide, you can block the video from playing. That said, you should be aware that not all video streaming platforms include this feature at all plan levels. Be sure to assess its availability on specific OVPs and plans you are considering.

A related security feature are IP restrictions, or geographic restrictions. This feature allows you to whitelist and blacklist certain countries. Therefore, if you only have a content broadcast license for a single country, you can whitelist that country and blacklist everywhere else in the world. This technology works based on IP address ranges, and it provides a great way to prioritize your target audience while blocking access for everyone else.

5 Time-Based Security: Video Scheduling and Signed Embed Codes

The next security features we'll cover are time-based features.

The longer a video remains public, the more likely it is that pirates and other hackers will target it. Video Scheduling is meant to address this issue. It can protect you from having time-sensitive, out-of-date content persisting in public, where it can damage your reputation or credibility.

Let's say you have a course available for a limited time only, or a deadline by which staff must have completed their health and safety training online. You set the time and date when you want your video to appear and disappear. No one can access the video outside the time frame you set.

Essentially, video scheduling allows you to make a video accessible for a window of time, and then close off all access after a certain amount of time has passed. This tool effectively uses a short time-access window as a security feature.

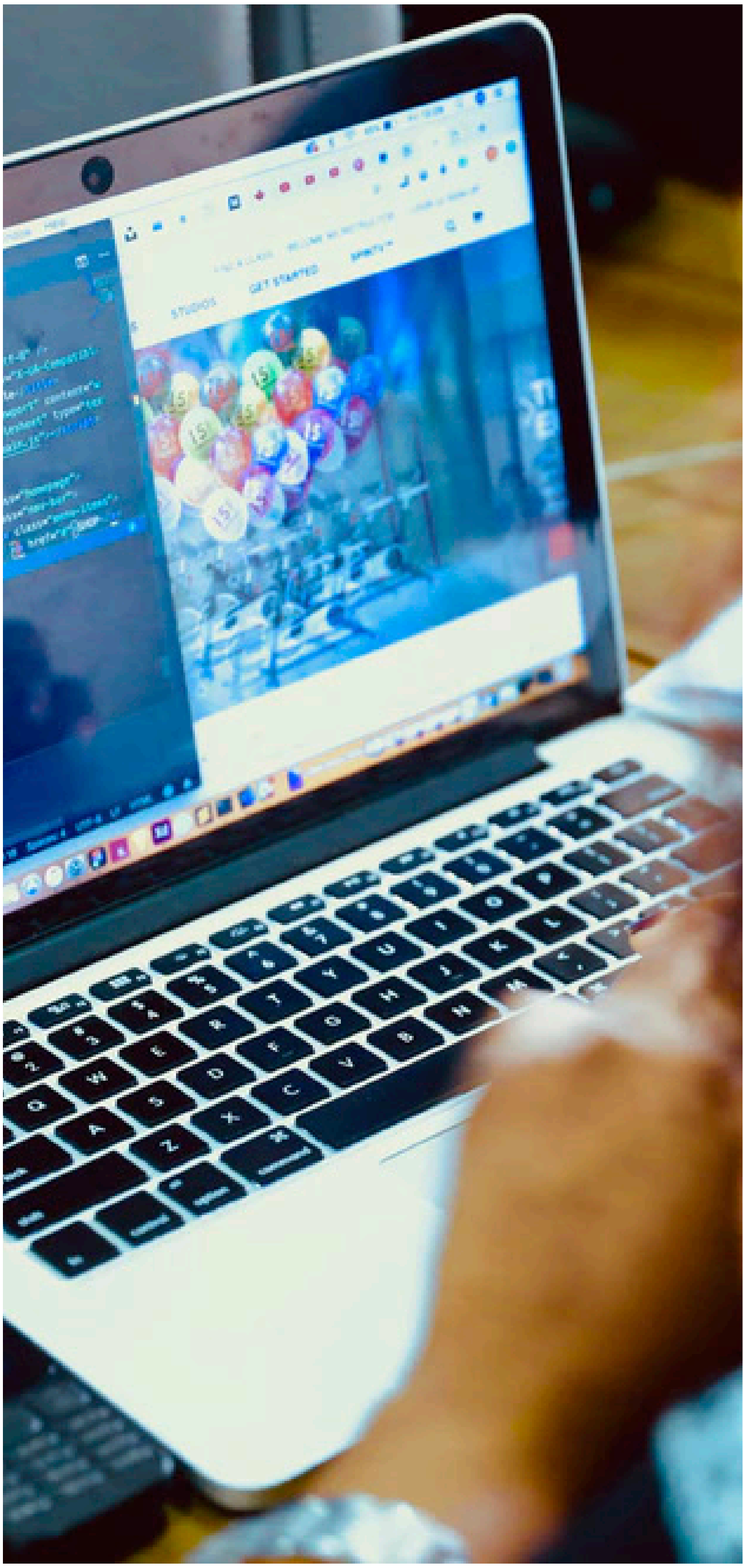
The second time-based security feature we'll highlight here are signed keys, sometimes known as tokenized access. Signed Keys are an extremely secure option that prevents third parties from embedding your videos without your consent. This approach uses secret signing keys with an expiration time to limit content access to authorized viewers.

Typically, Signed Keys are intended for use in applications that are dynamically generating HTML content. Signed Keys allow you to set an expiration time for your embed code, so that a particular embed code is only valid for a limited time into the future. When your application generates an HTML document with an embedded video, it also generates a signed embed code, specific to that page, which is only valid for a short time into the future. Note that if your pages are static, you cannot use the Signed Keys tool, as the key must be generated in real time.

6 Watermarking to Claim Your Copyright

Another method of protecting your content is watermarking. Watermarking refers to including a logo or text on your video, to ensure that ownership and copyright are clear. Watermarking can also improve your branding and professionalism. On the security side, watermarking prevents pirates and other scammers from copying your video and passing it off as their own.

Unlike social media video platforms that do not allow you to upload your own logo as a watermark, such as YouTube and Facebook, most professional secure streaming solutions offer this ability. However, like other features we've reviewed in this eBook, watermarking is not always available on all plan levels. Depending on your budget and your business needs, you want to pay attention to availability of this feature.



It's also usually possible to embed a watermark at the production level, using your mixing software. We highly recommend using watermarking for all of your content! It's a simple security feature that adds an extra level of security with almost no effort.

7 CDN Delivery for Scalability and DDoS Protection

Finally, let's talk about stream delivery. The ability to effectively deliver your stream to a large audience is a security issue. If you aren't ready to scale to thousands or millions of viewers, a surge in traffic can crash your stream and ruin your broadcast.

On top of this challenge, one of the most common hacking attacks today is called DDoS, which stands for Distributed Denial of Service. This attack typically uses what's called a "botnet"—a network of devices which hackers have taken over using viruses or other malware. In a DDoS attack, hackers unleash a botnet against a target website or online service, flooding their servers with millions upon millions of spurious requests. As a direct result, websites and videos can slow down and even crash completely.

In general, streaming quality is increasing. Video start failures are down 33 percent year-over-year, buffering is down 41 percent, and picture quality is up 25 percent. But this trend is not a given.

The best way to solve these issues is by using an online video platform that works with a large CDN, or Content Delivery Network. Ideally, this should be a "Tier 1" CDN—one of the backbone networks of global internet distribution. A Tier 1 CDN also typically has a large number of globally distributed "PoPs"—Points of Presence (for example, Akamai more than 239,000 servers in 139 countries worldwide). The large number of servers and sophisticated filtering technology helps defuse DDoS attacks, and geographic distribution ensures viewers get the best possible streaming experience no matter their location.

Which Security Features to Use at Which Time

Events, Publishing:

- Secure payment
- CDN delivery
- IP/Geo restrictions
- Signed Keys
- Scheduling

OTT:

- Secure payments
- Domain control
- CDN delivery
- Signed Keys
- IP/Geo restrictions

Internal communications:

- Domain control
- Signed Keys
- Password protection
- Scheduling

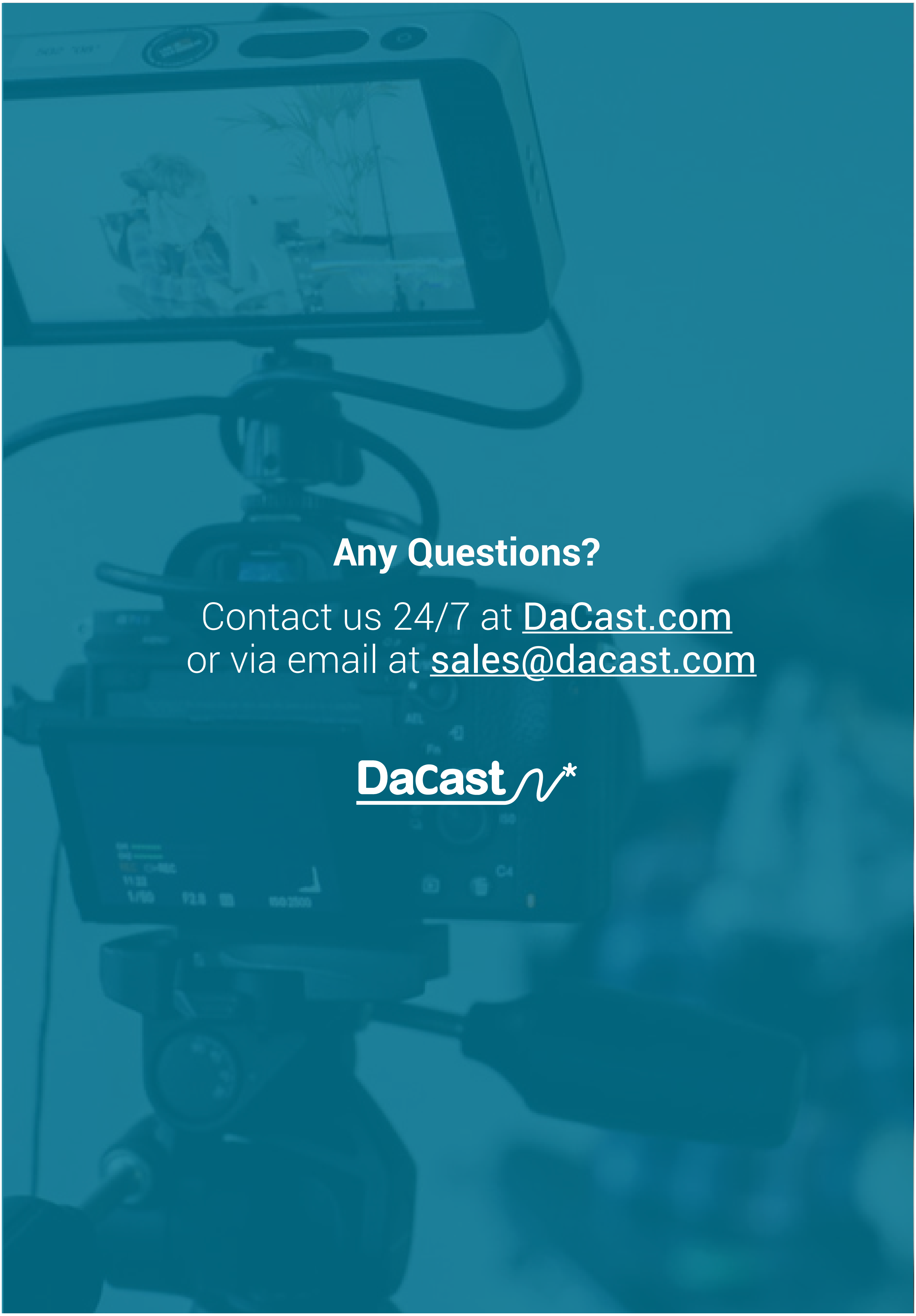
Choosing a Secure Streaming Solution

In a world with rapidly evolving threats and attack vectors, securing your online presence is paramount. While the world of video security can seem rather complex, in reality security tools are not too difficult to set up and use. A modern, professional-grade secure streaming solution will provide you with all the tools you need to get up and running quickly.

Prices can also vary widely. Some platforms provide features listed above for just $19 per month, while others charge $1,000 or more per month for plans including the same features.

DaCast provides all of the features discussed above, including encrypted video delivery, password protection, a secure payment system, domain and IP restrictions, video scheduling and signed embed codes, watermarking, and tier 1 Akamai CDN delivery. Whether you are looking for a secure live streaming solution or advanced video hosting platform, we've got you covered!.

If you want to know more about our advanced security streaming solutions and how we can help your business with video security hosting, contact us 24/7 or sign up directly to our platform.



Any Questions?

Contact us 24/7 at DaCast.com
or via email at sales@dacast.com

DaCast