

We frequently receive questions about the security of our streaming services. Video producers have copyrighted property to protect, and video licensees have a duty to honor producers' intellectual property rights. We make it a top priority to ensure both of these needs are met whenever implementing solutions for our clients.

Because we use Adobe Flash Media Server (and Wowza Media Server, which uses the same streaming protocols as Flash Media Server), there are a lot of security mechanisms in place merely due to the method of streaming delivery. Below are answers to a few frequently asked questions from [Adobe's FAQ page](#) which address most, if not all concerns relating to streaming security. It should be noted that since we provide true streaming, rather than progressive downloads, that the actual media files cannot be harvested using readily available tools. Most people are unaware that YouTube, Vimeo, and other competing providers don't do true streaming, but rather, progressive downloads, and this is why it is so easy to find tools to rip that content.

Is my content safe with Flash Media Server?

Simply streaming through Flash Media Server using RTMP, multicast, or RTMFP is one easy method to protect your content from download because media cache is deleted after it has been displayed. There are also several features built in to Flash Media Server that help ensure your video is available to a wide audience while still helping to protect the actual video files. Features such as real-time encryption, domain control, and video player verification (SWF file verification) help protect your content. Flash Access protection is also supported with all Flash Media Server 4 editions; find out more about Flash Accessprotection.

How does Flash Media Server protect from stream theft?

Streaming media using RTMP or RTMFP including multicast helps protect your content because media is not cached by the client. Streaming media using HTTP progressive or HTTP Dynamic Streaming can be cached.

To help further protect your content, you can use stream encryption plus SWF file verification.

Flash Media Server supports real-time encryption through RTMPE and RTMFP. It also supports delivery (over all protocols) of content protected with Adobe Flash Access™ software. Live HTTP streams can be encrypted in real time also using Flash Access.

SWF file verification (with RTMP) helps ensure that the video player accessing your video is actually your video player and not a modified or spoofed version of it. SWF file verification is also supported with content protected by Flash Access.

Does Flash Media Server support domain checking?

Yes, you can use domain whitelists/blacklists to further protect your content from unauthorized access. Multicast streams do not require server connections, so more advanced access controls will be required in the network or at the client.

What other content protection does Flash Media Server offer?

Using Flash Media Interactive Server or Flash Media Enterprise Server with server-side ActionScript®, you can verify that the client is authorized to play the video through a variety of metrics, including referrer, domain, IP address, or even Flash Player version. ActionScript can be used to manage requests made to Flash Media Interactive Server or Flash Media Enterprise Server. With all editions, you can protect SWF files from being reused or modified when using RTMP and help prevent unauthorized connections with SWF file verification.

C++ can also be used to manage authorization by creating custom plug-ins for Flash Media Interactive Server or Flash Media Enterprise Server. Plug-ins can be used to closely integrate into your network. You can also leverage databases or user management services such as LDAP using plug-ins. New with Flash Media Streaming Server 4, you can now create C++ access plug-ins (such as the Authentication plug-in for Adobe Flash Media Live Encoder software).

Media packaged with Flash Access protection can also be streamed with all Flash Media Server 4 editions.

