The Value of the KZO Video Suite

Today more companies are integrating video into their daily training and communication's processes. While embracing video can streamline communications in the workplace, the proper precautions must be taken before using video to transmit sensitive information within and outside the company.

There are three major areas of security concerns which need to be addressed with video before these tools are deployed.

The first major area to consider is streaming video versus progressive download. An enterprise must decide on how they intend to deliver their video to the end user before deploying a video solution. There are two viable delivery options to consider: streaming or progressive download.

Many users often assume incorrectly that if video is uploaded to a web server, only those users with permission will have the ability to view the content. In most cases, content is actually being downloaded locally to the user's computer. This local downloading of the video is commonly called progressive download. Many video platforms and web browsers work this way. YouTube is one of the most popular examples of a vide platform that uses progressive download. With progressive downloading, the video is downloaded locally onto the viewer's computer as it is being watched. This can be seen with the red bar progressing as you watch a YouTube video. Once the video has been viewed, the viewer can access their computer to retrieve the video file and take ownership of it without being granted the proper permission.

Video streaming technology can be used as the secure alternative to progressive downloading. When a video is streamed, the server is only sending the viewer the data bit by bit. When a streaming video is viewed, roughly 3 to 5 seconds of that video is sent to the viewer's computer and the content already viewed is deleted. Therefore, with video streaming, the video is not downloaded to the user's computer because the viewer will only have 3-5 seconds of video stored on their computer at any one time. Since the video file is not stored on the user's computer, video streaming is the more secure delivery option.

The second area to consider is SSL or Non-SSL Delivery. An enterprise can deliver content over Secure Sockets Layer (SSL) instead of choosing to deliver content in HTTP or clear text (non-SSL). For example, traditional YouTube videos are delivered over HTTP, with the data flowing in clear text over the network. This means that anyone listening in on the network has the ability to see any content that those with permissions might be viewing at the time. In other words, anyone using the same network can "see" the videos that you are viewing on your computer. This is commonly referred to a "man in the middle" attack.

For secure delivery of content, stream the video content over Secure Sockets Layer (SSL) and the data stream will be encrypted between the server and the end user's computer. With SSL delivery, if anyone "sees" the content, they will not be able to decipher it because of the data encryption. Any previous steps taken to secure video content will prove irrelevant without the information being delivered with SSL.

The third area to consider is a Rule and Role-Based Permissions Systems. The enterprise can add another layer of security to their content by setting the proper access controls. These controls give those responsible for the content the ability to control who can see what video content, when they can see the video, and what they can do with it like updating. Groups are already defined within an enterprise and videos are often relevant to specific roles or departments in most organizations. An enterprise should choose a video solution with a rule and role-based permissions system that can seamlessly tie into their organization structure to set access controls. When used correctly, a rule and role-based permission system can ensure that video content is only being viewed by the people who should have access to it.

The KZO Video Suite and Video Security

The KZO Video Suite offers security features to enterprises that address all of the security issues outlined to ease user concerns before leveraging on-demand video to disseminate information to your employees.

The KZO Video Suite offers the following security features:

1. Streaming Video

The KZO Video Suite streams video content to users so that video cannot be downloaded and content only reaches its intended user or group.

2. Access Controls and Permissions

KZO enables the enterprise to set access controls to limit who can view the video content. . The enterprise can control access to videos based on a rule or role-based permissions. In addition, they can set access permissions to public or private/restricted viewing. They also have the option of requiring user registration - requesting information about the viewer before they are given access to video. The other benefit of the KZO Video Suite's access control system is metrics tracking. With KZO, the viewing metrics of each video can be tracked and reported to the content owners.

3. External Authentication

The KZO Video Suite ensures sensitive information is not leaked to external sources. The KZO Suite can be integrated with existing authentication and security systems such as LDAP, Active Directory, and Single Sign-On. This integration enables the KZO Suite to be used across the enterprise with users authenticated using their current credentials.

4. Safe Delivery over SSL

The KZO Suite can stream video content over Secure Sockets Layer (SSL). With SSL, the video content is encrypted and will remain secure while it is delivered to the user.

If the video is delivered to the viewer without using a series of protective security features like those offered by KZO Video Suite – then it is possible for the enterprise to lose control of their video content.