Enterprise Video Security Components & Services
Introduction
Enterprises have rapidly adopted cloud-based services for their IT needs in an effort to reduce ongoing infrastructure costs. In recent surveys, as many as 87% of respondents had indicated adopting public cloud services. This includes adoption of services processing and housing mission critical data like CRM (Customer Relationship Management), ERP (Enterprise Resource Planning) and traditional office applications, as well as the growing volume of enterprise video communications.

When considering a video streaming solution, it is important to ensure content is protected. This is especially true when the streaming solution is cloud based. We’ve heard the nightmare stories of compromised customer information. Video is just as important and potentially as sensitive as any other content type for many of our customers.

This paper will itemize the essential security components that should be considered when adopting a cloud-based service, and IBM Watson Media platform capabilities for each of those components. Topics covered include authentication, authorization, role-based administration, encryption, content protection, and data backup procedures. These are the core factors to consider when selecting an enterprise video streaming solution.

The core focus of this publication will be on the IBM Enterprise Video Streaming solution. However, role-based administration, encryption, content protection, and data backup procedures apply to the external Streaming Manager solution as well.

Authentication
The first step in content protection is to define the set of users you want to access your content. Enterprises typically want to restrict access to their employee base. This is generally defined through a user directory such as LDAP, Google Apps Global Directory or Microsoft’s Active Directory. These directories contain user ID’s and passwords, along with other enterprise data. The point of authentication is to validate that a user is who they say they are. This is done by mandating the entry of a valid login and password combination. If a user with a company ID enters the correct password as defined by the directory, then we consider that user authenticated.

Additionally, a widely deployed technology is Single Sign-on (SSO), which is projected to be used by 86% of SaaS (Software as a Service) based solutions and needed by 80% of enterprises. With this technology, a user is able to authenticate once to a central service. From then on, that user will be granted access to authorized services for a pre-defined period of time without having to re-enter their credentials. There are various methods of implementing a SSO solution but one of the more prevalent, especially for cloud services, uses a technology called SAML (Security Assertion Markup Language). With SAML, an enterprise shares their authentication status for an internal or Internet based user via a publicly accessible service referred to as an Identity Provider or IdP. The IdP allows the browser to pass on the user’s authentication status to the Service Provider.

IBM Watson Media fully supports SAML 2.0 implementations and has thorough integrations with some of the leading providers of SAML technology, including: Okta, Ping, OneLogin and Google Apps for Work. This integration means that users won’t have to enter their credentials when attempting to access IBM Watson Media if they are already authenticated. If they aren’t authenticated, the user will be redirected to their SSO service to provide their credentials. This means that IBM Watson Media will not receive or store any user passwords. Beyond being a security benefit, this also benefits the end user as well through reducing the number of unique logins they will have to remember. This offers an improved experience for those accessing this content and also a decrease in costs, as it’s projected that 30% of help desk enquiries are regarding the reset of a password someone forgot.
Authorization

Authorization allows for content to be accessible to a specified set of users. This is also referred to as “access control”. For example, you may want to allow everyone within the company to access a recording of the latest corporate all hands meeting; however, you may want to restrict access to a video on a new product, still under development to specific teams until elements of that product are finalized.

With IBM Enterprise Video Streaming, this is simple to setup and to accomplish. Authorization is controlled at the Channel level. At IBM Watson Media, a Channel is a grouping of content. This includes one live channel, whose use is optional, and a series of VOD (Video On-Demand) files. Authorization is an important function of the Channel within the IBM Watson Media platform, in addition to organizing content for viewers. The beauty of the IBM Watson Media solution is that existing AD or LDAP group definitions can be used to define the scope of access to the content in a Channel. For example, if there is already a directory group corresponding to the executive team, that group name can be associated with a Channel called the Executive Channel, or another name of the enterprise’s choosing, to limit access to just members of the executive team. In addition, you have the flexibility to associate one or more groups and individual users to the access control list.

This authentication access, especially in the context of a group of employees, is continually updated. For example, in the event we receive notification from the SAML authentication that someone has left the organization we can disable playback access for that individual within milliseconds.
Role Based Administration

In large organizations with complex applications there are often multiple administrators to distribute the workload. This is important not only from a work distribution perspective, but also prevents having to depend on a single employee in the event of an urgent administrative need. The concept of role based administration allows multiple administrators without having to give a superuser administrative account to each person individually. You can therefore limit the control of an individual admin.

IBM Watson Media supports multiple admin roles with different functionality. The Super Admin is able to perform administrative tasks across all areas of the account. Super Admins can delegate admin tasks to Channel Administrators. Channel Administrators, on the other hand, are able to perform these administrative functions within one or more Channels, rather than across the account. With IBM Watson Media, you are able to assign one or more Channel Administrators. These administrators can also preview unpublished on demand content, viewing and implementing cloud based trimming before assets are viewable by others.

Additionally, the Moderator role is associated with live events. One or more Moderators are able to manage incoming questions that are submitted during live events. This can range from controlling the visibility of questions to answering them.

Encryption

The purpose of encryption is to prevent snooping attacks where content can be accessed with network tap and sniffer technologies and is critical when content is on the wire. To address this, IBM Watson Media supports encryption of encoded streams using AES (Advanced Encryption Standard) 128 encryption. Content that is encrypted with AES 128 is limited so that access requires being decoded by authorized players in browsers where the stream is delivered using HTTPS (HTTP over SSL/TLS). This is done through symmetric-key algorithm, which means the same key is used for both encrypting and decrypting the data.

IBM Watson Media allows users to access the viewer and admin portals using HTTPS, the encrypted version of HTTP. In addition, the video stream itself can be delivered using HTTPS. This is especially important if the player is embedded into a web page that is delivered via HTTPS.

HTTPS is an application of SSL (Secure Sockets Layer) or TLS (Transport Layer Security), which is capable of securing transmission over TCP. While the two terms are used interchangeably, TLS is actually the successor of SSL. In fact, TLS was built from SSL 3.0. While the initial offering of TLS was noted as “marginally more secure”, the technology has advanced. Furthermore, major exploits have been discovered in SSL 3.0, noted publicly by Google and Mozilla, leading to it being disabled in some browsers. Consequently, IBM Watson Media uses TLS encryption methods for data in transit. In execution, this works through encapsulating all communication between a client’s or viewer’s machine and the server through four protocol layers of the SSL protocol. These four layers include: Record Layer, ChangeCipherSpec Protocol (signals the beginning of a secure communication), Alert Protocol (sends errors, problems or warnings about the connection), and the “Handshake” Protocol.

The first and last protocols allow the client to authenticate a server and establish an encrypted SSL connection. This involves the server presenting its digital certificate to the client’s machine to authenticate the server’s identity. This process utilizes public-key encryption to validate both the certificate and to confirm the server’s identity claim. Following a successful authentication, the client and server establish a cipher setting and a shared key to encrypt information that is exchanged during the session. This process is nearly invisible to the end user, although they will see a padlock icon appear in their browser URL bar to confirm the process was successful.

Use of HTTPS allows IT to maintain their standard supported firewall port of 443 rather than requiring the use of a non-standard ports like 1935 (RTMP, Real Time Messaging Protocol) or 554 (RTSP, Real Time Streaming Protocol).

![Figure: AES encryption](image-url)
Protecting Video Streams

Another security element for organizations to consider are ways to protect their video streams from being rebroadcast on unapproved sources. This can include video players on other websites that show a live or on demand stream without consent.

IBM Watson Media protects against this in several ways. On an inbound RTMP stream, someone trying to hijack a stream would need to know exactly when an organization is streaming plus the RTMP URL and StreamKey, the latter of which is randomized. Plus they would need to grab each packet which would be routed multiple ways to IBM Watson Media’s ingest point and then be able to reassemble into the proper order.

On an outbound RTMP stream, we transcode videos to a proprietary format. This prevents other, third party players from accessing and rebroadcasting this stream. Because playback is restricted to the IBM Watson Media player, tools are available to prevent others from copying that embed code and placing it on undesired webpages. This feature allows content owners to restrict embed URLs to a single web page, several web pages, or an entire website domain.

IBM Watson Media’s intelligent player, which can change between CDN sources in a millisecond, are constantly receiving information back from those viewing it. As a result, when a player is embedded we can detect exactly where the video player is located. If a detection is made that the player is on a cloned or unapproved site, it can be disabled in a few milliseconds.

Other Security Considerations

Any public facing web application should also protect against the top Open Web Applications Security Project (OWASP) security vulnerabilities (https://www.owasp.org). While there are tools on the market that offer a layer of protection against these types of attacks, ideally the web application is designed to inherently prevent these vulnerabilities.

IBM Watson Media tests its site against OWASP attacks using Penetration or PEN testing. This is an important measure to protect the site so it does not get hacked. As a result, daily vulnerability and penetration checks are run through Nessus scans. IBM Watson Media has also passed several external audits from companies such as KPMG as part of vendor assessments.

While we think of SaaS solutions as being in a cloud, ultimately the servers and storage of content is in a physical data center somewhere. These physical facilities need to meet the highest standards for security including access control and monitoring. The relevant standards assessing this are SOC 2 and ISO 27001. SOC-2 stands for Service Organization Control 2, and compliance validates that an organization has passed a security audit that included a stringent evaluation of virtually all of their relevant processes, procedures and controls for data protection and availability. ISO 27001 prescribes 14 information security domains that consist of 114 security controls for the security of information assets. IBM Watson Media data centers comply with these standards.

Figure: Embed restriction example
Data Backup and Recovery
Securing content is one part of the equation, but protecting content in the event of the unpredictable is another. As a result, IBM Watson Media practices rigorous data backup and recovery processes to protect data and stored content if the worst should happen. This includes the ability to recover data when needed.

To execute on this, we conduct full, daily backups of core components and data. These components include the following: database, codes, server configurations. VODs are stored through multiple independent storage, with backup achieved by data redundancy. In addition, daily restore verification processes for the database are done to verify that the backup process is functional and that the restores work. There is an instance for non-critical reporting purpose which is loaded from backup on daily bases. In addition, the infrastructure team gets email notification if any of the backups fail.

This backup process, as it relates to media used, is also protected through making sure this media is rendered unreadable at the end of its useful life. As part of the backup cycle, IBM Watson Media uses hard disk drives for backup purposes. No other media, such as DVD or tapes, are utilized. At the end of the lifecycle of a device the data is wiped by Linux's standard “wipe” command. Before any backup media is reused, data contained on them is fully destroyed through using DBAN (Darik’s Boot And Nuke).

Backups are protected from unauthorized access and tampering as they are physically separated in the data center. Furthermore, backup file access is limited to authorized personnel from our infrastructure team.

While the backup process mitigates risk, sensitive video data is also disposed of when no longer needed. As a result, video content is deleted at the backup level after seven days of being deleted by the enterprise from inside their account.

Conclusions
When evaluating a video streaming platform for its features and functions, an analysis isn’t complete without also considering whether the content it contains will be protected. Moreover, the solution must work with existing, security standards and technologies like SAML, LDAP and HTTPS. Whether it be corporate communications, training, marketing or HR, video is becoming a significant content type for businesses of all kinds. Are you managing it with the same rigor as other content types? By selecting a video platform that has comprehensive security capabilities, you’ll avoid exposing your organization to unnecessary risk.
About IBM Watson Media
Created in January 2016, IBM Watson Media brings together innovations from IBM’s R&D labs with the cloud video platform capabilities of Clearleap and Ustream. Through the unit, IBM delivers a powerful portfolio of video services that spans open API development, digital and visual analytics, simplified management and consistent delivery across global industries. IBM Watson Media supports top media and enterprise companies with reliable video on-demand and streaming services.

For more information on IBM Watson Media, please visit www.ibm.com/watson/media.

Footnotes


