WHITE PAPER

amagi

Ensuring content security with CLOUDPORT channel playout platform

Srividhya Srinivasan
Co-founder, Amagi

www.amagi.com

Introduction

Amagi CLOUDPORT moves entire playout to a secure public cloud. The cloud-based playout model helps TV networks improve their broadcast ROI, launch and localize channels on the go, and address disaster recovery needs cost-effectively.

Managing broadcast operations can be challenging with traditional models due to their slower time to market, high CAPEX and OPEX, and lack of flexibility to localize channels or scale operations efficiently.

Amagi has built a next generation cloud - based playout platform that can be used to launch and operate channels over satellite, cable, IPTV and OTT. CLOUDPORT is a comprehensive end-to-end platform suitable for 24x7 playout for live and non-live channels.

CLOUDPORT can be set up either as a playout on the cloud or be deployed at the headends as edge playout platform. The entire system can be managed remotely using a Web-based UI.

Amagi's CLOUDPORT infrastructure encompasses

Content preparation servers (Transcode & Transport servers)

Web based playout management tools

Cloud-based backbone for content delivery, management, and monitoring

CLOUDPORT playout server

This white paper discusses the security requirements for content broadcast, and how Amagi's CLOUDPORT platform is best positioned to address them.

Security requirements for content broadcasting

Security needs related to content broadcasting have to be thought through from an end-to-end system perspective. The key requirements are:

- All media content is secure from any unauthorized access.
- Media on the Playout Server is completely protected, including but not limited to the willful hacking of the Playout Server by third parties.
- End-to-end chain starting from TV network facility to Playout Servers is inaccessible for public access, and is secure from any attacks - willful or otherwise.
- Public cloud providers and third-party service providers do not have access to media content, except when provisioned by the TV network on its behalf, for specific operational requirements.
- Robust and secure login, administration and approval procedures are in place to protect TV Network operations. All related content is protected against unauthorized access by employees and tertiary staff inside the TV network's premises.
- The system is expected to have security audit trails and logs for post-incident analysis and periodic review procedures.
- The digital identities of all service providers and devices at affiliate headends are authenticated, and remain genuine over the lifetime of the service.

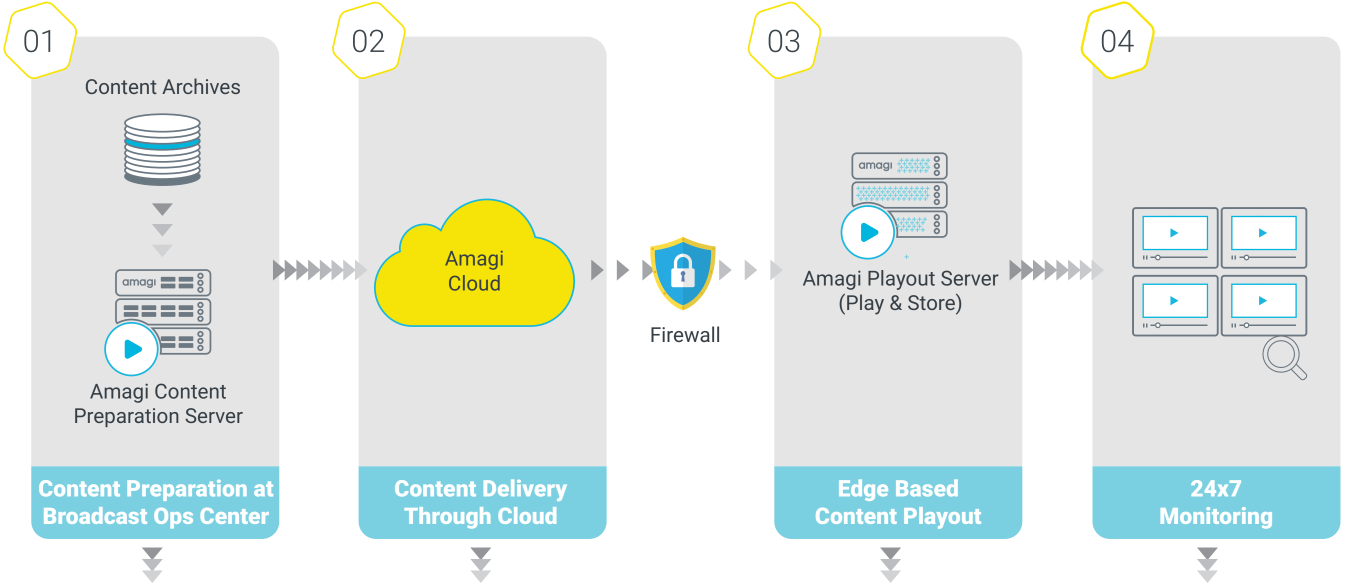
Amagi's security framework

Amagi has created a security framework to address the aforementioned security requirements for content broadcasting.

All media content is secure from any unauthorized access.

CLOUDPORT uses multiple layers of security to prevent unauthorized access to content. For ingest and upload to the cloud, content is encrypted using AES-256 bit encryption. CLOUDPORT uses ExpeDat, (A solution similar to Aspera or for fast file transfer.)

Know more about ExpeDat: http://www.dataexpedition.com/expedat/


01
Content Archives
amagi
Amagi Content Preparation Server
Content Preparation at Broadcast Ops Center
02
Amagi Cloud
Content Delivery Through Cloud
Firewall
03
amagi
Amagi Playout Server (Play & Store)
Edge Based Content Playout
04
24x7 Monitoring

- AES 256 bit encryption for transport to cloud

- AWS security infrastructure
- SSL & role based rights
- Authentication
- Isolated instances for storage, application & database for each customer
- AES-256 bit encryption for content

- 128 bit TEA content
- encryption
- Secure embedded Linux
- SSL
- Firewall

- Authentication
- SSL

On the cloud, each customer has **a separate and isolated instance for CLOUDPORT Web Application, Database,** and **AWS S3** and **Glacier Storage**. Content residing on the cloud storage is secured using **AES-256 bit encryption.** This prevents shared access to data and any consequent impact. Administrative access to these instances is exclusively available to authorized Amagi personnel.

The CLOUDPORT application uses **role based user access management rights** for its various features, thereby ensuring authorized access and action for content, schedules and playout. For example, a user with Scheduler rights has no access to download/upload content. The content is transported utilizing either SSL or secure **Expedat** content transfer protocols.

On the CLOUDPORT Edge Playout Server, content is encrypted and stored using 128-bit encryption. During playout, in-memory runtime decryption is done for a 128-bit block size, which is subsequently played out.

Media on the Playout Server is completely protected, including but not limited to the willful hacking of the Playout Server by third parties.

The final SDI output of playout is presented for further processing by a distribution plant. No access and visibility to the media files or schedules is provided, as the content is stored as AES 128-bit encrypted files on the playout server, ensuring that the content is not retrievable even if the storage units of the playout server are physically removed.

All CLOUDPORT playout server operations are automated, and do not require operator assistance other than for standard remote functions (e.g. Power On/Off). The playout server incudes proprietary hardware and software, which can only be administered and operated by trained Amagi personnel.

All communications from the playout server to the cloud (including content download) occur over an encrypted private VPN connection to the AWS cloud instance.

The playout server runs Secure Embedded Linux, which is configured for highly secure remote access by Amagi's customer-specific support team over an encrypted VPN tunnel.

At the application level, access-rights based on roles prevent the access and modification of any content or schedule.

End-to-end chain starting from TV network facility up to Playout Servers is inaccessible for public access and is secure from any attacks willful or otherwise.

The end-to-end CLOUDPORT system comprises of the Content Preparation Server used for provisioning content to playout, cloud based application, content storage on the cloud, and the edge-based playout and monitoring servers.

The Content Preparation Servers at any given broadcaster's facility receive content in the broadcaster's preferred choice of file format before transcoding and uploading that content to the AWS Cloud. The Content Preparation Servers are located within the TV network facility and adhere strictly to the TV network's Information Security policies.

The CLOUDPORT application, content and databases reside on the highly secure AWS Cloud, with security policy that covers platform, access controls, processes and audits for Network Security.

Further information about Amazon's AWS Security Policy:
https://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

All devices connected to the cloud are protected by enterprise grade local firewalls (Configured by Amagi), which are not accessible via external internet-enabled networks. Authentication systems are used for accessing real-time IP streams for video-monitoring and maintaining compliance archives.

The playout server communicates with the AWS Cloud using a secure VPN tunnel which is configured to allow connections exclusively from the Amagi-AWS Cloud instances.

Public cloud providers and third-party service providers do not have access to media content, except when provisioned by the TV network on its behalf for specific operational requirements.

All content stored on the cloud is encrypted, and the keys are generated and made available only for the CLOUDPORT application, based on the actions of users with access rights. Access rights are never shared with public cloud providers and/or third-party service providers.

Robust and secure login, administration and approval procedures are in place to protect TV Network operations. All related content must be protected from unauthorized access from employees and tertiary personnel inside the TV Network's premises.

Amagi's managed services and employees are governed by a well-defined Information Security policy that encompasses the information security management processes, organization, content security, access controls, physical and environmental security, communications security, and systems security.

The system is expected to have security audit trails and logs for post-incident analysis and periodic review procedures

CLOUDPORT maintains highly detailed audit logs at both system and user access levels. Consequently, user actions can be traced for post-incident analysis or procedural reviews.

The digital identities of all service providers and devices at affiliate headends are authenticated and remain genuine over the lifetime of the service.

The CLOUDPORT servers and devices communicate over SSL, thereby ensuring encryption of all traffic. By design, playout servers (devices) can be configured exclusively by Amagi, utilizing identities and tools that are never disclosed to end-users. These devices use proprietary handshakes and authentication APIs for sourcing of content and playlists, thereby preventing any unauthenticated access to the system.

Moreover, the support team constantly monitors devices and the system for all activities, including internal system processes. This puts any extraordinary activity under review.

Conclusion

By design, Amagi CLOUPORT has been built as an end-to-end secure system. The system uses existing, time-tested and standards-based approaches to security to ensuring enterprise grade security for all broadcast operations.

About the author

Srividhya Srinivasan is one of Amagi's co-founders, and heads technology and operations for Amagi. She is a passionate technologist and leads new product development and engineering at Amagi. A stickler for precision, she is responsible for ensuring that Amagi stays one step ahead of the curve.

amagi

Amagi is the world's first cloud-managed broadcast services and targeted advertising solutions company. Amagi brings simplicity, advanced automation, and transparency to the entire broadcast operation, be it for traditional TV or next-gen multiscreen platforms. Amagi has deployments in over 40 countries, enabling TV networks to launch, operate, and monetize channels anywhere in the world. Amagi also provides targeted advertising solutions to 2,500+ brands, shaping the future of TV advertising. Amagi Corporation is based in New York, with offices in London, Hong Kong, New Delhi, Mumbai, and the R&D center in Bangalore.

cloudandme@amagi.com