

amagi

An Amagi Point of View  
December 2021

# Want a secure broadcast workflow? Move to the cloud



# Media & entertainment: the journey to a digital mindset

*"No way am I going to put my content on a server I don't own. Let alone one whose location I don't even know!"*

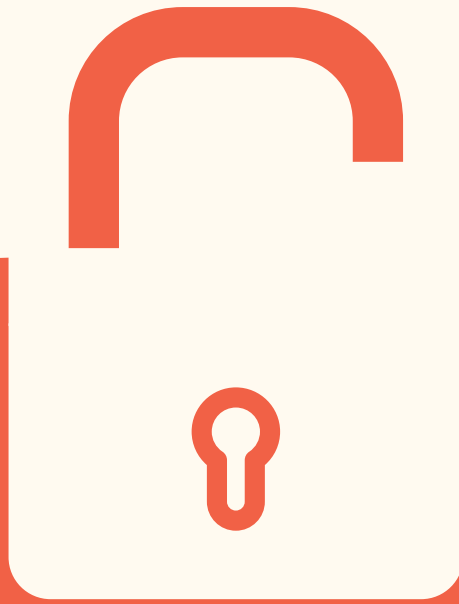
That was certainly the ready response of many broadcasters and media companies a decade ago when the possibility of cloud-enabled workflows was introduced to the media industry.

Even until fairly recently some industry professionals regarded safety in the cloud with an almost superstitious anxiety, convinced that the safest place for their content was under their own roof. Thankfully, the tide is turning on this fallacy, and while there's no reason you can't keep your own content secure on your own premises, with the most powerful media companies in the world trusting their assets entirely to cloud, a new paradigm is emerging.

Media production became, over the twentieth century, one of the cornerstones of modern civilization. Broadcast centers were built in major cities, which housed business, production, transmission and resources all under the same roof. Film studios were the same - like walled cities of old with everything from catering to finance to tech research happening under the control of one head who ruled the studio like a king.

As media moved into the 20th century, these structures were digitized, and economics encouraged more outsourcing, but the principle of keeping your key assets within your own brick and mortar facility remained.






## The anxiety of letting go of your content: Security concerns & fears

Historically, broadcasters had all their content, with their processing and the distribution models, all on premises. They were comfortable with the physical proximity of everything they did, whether it was the processing, the content, or the controls that they needed to access.

Moving to the cloud was a physical separation between the content and the operators. This anxiety was similar to the early days of banking, when people moved their money from under their mattresses to a locked building run by people they didn't know.

Content is the crown jewel of any media company and so the same sorts of security conscious conversations played out in content businesses when cloud storage – and later, fully cloud-based workflows – were introduced.



Coming into the cloud fresh, there was anxiety about identifying all the potential threats.

- **Control access:** The first concern was being able to control access to the content. To use the bank analogy – how can I be certain that someone with a six-shooter and a black hat can't just walk into the bank, say he's me, and ride away with my money?

And how can I access from within my organization. How can I make sure that editors have access to all the assets they need, but still keep them protected from a well-meaning assistant.

- **Encryption & security:** Beyond ensuring that kind of user authentication, will the content be encrypted and secured to a point that if it does get into the wrong hands – is stolen by hackers, say – that the material can't be used or accessed in any meaningful way without the proper permissions.

As playout from the cloud became a viable option, a new set of anxieties reared their heads.

- **Reaching the right audience:** When content finally leaves the cloud storage and heads off through an IP pipe out into the public internet, how do you know it's going to the right people – the right subscribers, the right territories, the right content partners?
- **Monetization:** How can you be certain that it's getting monetized via the proper paying customers and the right advertising?



## Let cloud do the lifting

In recent years, the security fears have given way to an understanding of the benefits of public cloud.

**With the basic hygiene of creating the right security processes and using the technologies that are widely available today, public cloud is the most secure environment in which to place something.**

The sophistication that the public cloud vendors have built in terms of security infrastructure today, are far, far higher than what a company, or even the data center of a particular company, can match. So, stealing content directly out of the cloud is an inherently difficult proposition.

**A recent [article](#) published by SMPTE observes that public cloud providers are now actively adapting tools for the needs of the media industry.**

**When public cloud is prepared to court major institutions like film studios you can trust that you're dealing with a very secure environment.**

- **Cloud providers are continuously upgrading security protocols and threat detection.**

They are continually addressing security issues that would be expensive, and exhausting, for an individual organization to deal with alone.

- You also have the option of picking the right design considerations to build a highly resilient cloud infrastructure. **Go for multi-cloud environments or instead pick a single cloud provider but multi-region**

You can get flavors of diversity in cloud infrastructure that helps deliver more uptime and security capabilities. With cloud, you can thus enjoy the benefits of seamless redundancy infrastructure. Content can be striped across multiple data centers in multiple regions and zones, which makes it theoretically unlosable – as well as making it more difficult to steal.

- **Machine learning is becoming a core component of cybersecurity across industries.** Sets of rigid rules which used to be the core of threat management, have given way to a flexible approach which – like some kind of cyber-tai chi – can flow and adapt to security threats that may take many different shapes.

Because of its access to scale, a public cloud provider is able to access large amounts of security data, which can then be used to train machine learning-powered security protocols.

Operators of an on-premises data center may be able to access a wealth of analytics and personal experience to keep their systems safe, but a cloud provider has access to exponentially more data on threats, as well as computing power to devote to combating them.

Threats come in different forms, and patterns have to be recognized and learned. A larger infrastructure like the cloud can learn threat management and detection much faster, because it has access to the whole breadth of signatures and patterns threatening the system.



# ALERT!

## Cybercriminals at the gate

Cyberthreats are very real, which is one reason it's good to have a powerful ally in fighting them. Because cyberattacks happen in the world of ones and zeroes, we can sometimes forget about how ubiquitous they are, but if we were to see them embodied in the same way as more traditional crimes, the world outside our window would look like Mad Max.

**Port scanning:** Opening one network port for a few minutes will invite literally millions of attacks. Cyberattacks are a fully automated 24/7 activity, with hackers searching the internet for open ports and access to systems. This is the equivalent of a thief trying every car door on a street to see which one has been unlocked, but on an enormous, relentless scale.

**Cyberattacks are like a spray across the whole world of IP addresses, and with a vast system supporting it on the backend. But a large part of the solution is about the discipline, not the technology. It is the human element that is the weakest link in this whole value chain. It comes back to processes. What processes can you put in place?**

## Best practices and proper protocols: The Amagi advantage

At Amagi we work with 2000+ linear channel deliveries and 800+ playout chains, so we take a lot of precautions.

**Our playout is run on hardened systems and we are inside VPC (virtual private cloud) rings,** so we are not open to the web. All the data and content are encrypted at rest and encrypted during transition.

**Amagi has also begun to initiate Security Information and Event Management (SIEM) processes.** SIEM is an approach to security that combines software products and services to provide real-time analysis of security alerts generated by applications and network hardware.

- The method first focuses on prevention of security breaches through a proper set up of technologies, processes and human resources.
- The second part is the focus on detection of threatening activity that is occurring, ideally before it ever can become an issue of concern.

**A 24/7 security operations center (SOC) has been established by the company, which monitors anomalies and can make predictions of the outcomes of any hacks.** Like any security team, the Amagi SOC runs simulations of threatening scenarios to practice and refine the best methods for defense and, if necessary, disaster recovery.





## Managing the challenge of APIs

With all this security in place, the easiest route for a cyberattack would be through a rogue customer account or operator, which again underlines that the principal vulnerability in your cloud strategy is internal permissions handling and workflow processes, rather than technology.

But no business exists in a vacuum. Your company may be meticulous in its cybersecurity protocols, but you are interfacing every day with companies who may not be practicing the same diligence – or even have an awareness of the threats. The industry is interconnected through multiple API environments, and APIs can be a point of weakness. In the case of APIs, security is generally based on shared tokens. If these tokens aren't managed well, or have a long lifespan, they can open the system to hacking.

**One way of solving the problem is to hit it with the largest hammer possible – with everything running on a VPC or behind a firewall – and handshake through a single interface.** In this scenario you avoid multiple APIs tentacling into your system.

# Need for a concerted approach

This tightly protected castle is very secure, but it isn't very scalable. The content ecosystem needs to remain flexible and maintaining both flexibility and security will require ongoing collaboration among industry bodies. Developing and evolving sets of API standards and guidelines across the sector will help create a safer environment for everybody.

Something as simple as a denial of service attack on APIs can be really devastating. To have some of these best practices qualified as a standard is going to make the industry much healthier. At present, however, there still is no base standard that third parties need to comply with.

Nevertheless, **Amagi develops every one of its cloud products and services with security in mind right from the initial design stage.** Enterprise customers are regularly presenting the company with security questionnaires and queries about processes, but with Amagi's redoubled focus on security, companies will now have the reassurance of the company's SOC 2 certification from the get-go.



# Security: In your hands

The industry may have accepted that the cloud is a secure place to store content, but it's good to know that some companies are making sure your entire cloud business stays secure. **Hygiene and security processes, not technology, is the most important factor in cloud safeguarding today.**

The good news for companies that still have anxiety about losing control security control in the cloud, is that it is still in-house expertise that controls the level of your content security. The content may not live under your roof anymore, but the security around it is still entirely in your hands.

**Read our Whitepaper for in-depth understanding of how Amagi ensures content security with Amagi CLOUDPORT**



# Thrive with us!

To move to the cloud using our unified broadcast workflows and stop worrying about content security, reach us at

[cloudandme@amagi.com](mailto:cloudandme@amagi.com)

## About Amagi

Amagi is a next-gen media tech company that provides cloud broadcast and streaming TV solutions to TV networks, content owners and streaming TV platforms. Amagi enables content owners to launch, distribute and monetize live linear channels on Free-Ad-Supported TV and SVOD platforms. Amagi also offers 24x7 cloud managed services bringing simplicity, advanced automation, and transparency to the entire broadcast operations for traditional TV networks. Amagi delivers 500+ channels with deployments in over 40 countries. Amagi has offices in New York, Los Angeles, London, Singapore, New Delhi and Bangalore.

[www.amagi.com](http://www.amagi.com)

The Amagi logo is centered in the lower half of the page. It consists of the word "amagi" in a white, lowercase, sans-serif font. Behind the text are two large, flowing, curved lines that sweep across the bottom of the page. One line is a light cream color and the other is a darker, muted red. They overlap and curve around the logo, creating a sense of motion and elegance.

# amagi