Publication date:
May 2021

Authors:
Rik Turner
Kedar Mohite

Ahead in the Cloud

What every entertainment professional should know about cloud security adoption

In partnership with:

OMDIA

verimatrix™
DRIVING TRUST

Brought to you by Informa Tech

Contents

Summary	2
IaaS, PaaS, and SaaS defined and sized	3
The benefits of cloud adoption for media and entertainment	7
Cloud security	9
TV and video service providers are at the center of the connected app economy	11
Distributed infrastructure demands hyperscalable security	14
An evolutionary model for cloud security	17
Conclusion	18
Appendix	19

Summary

Over the last decade cloud computing has evolved from a significant new method of provisioning enterprise technology to a cornerstone of delivering IT functionality and content to employees, business partners, and customers. Many companies now adopt a “cloud-first” approach, whereby any new application they plan to introduce will be deployed by default to the cloud unless its business owners make a very strong case for why it needs to sit “on premises,” that is, in the corporate data center.

Equally, startup companies across multiple vertical markets are these days often described as “cloud natives,” or “born in the cloud,” meaning that they came into existence assuming that all the applications underpinning their business processes would be cloud based. Add to this the fact that an ever-increasing proportion of customer interactions across the globe are online, and that the customers themselves may be located anywhere around the world, and the power and potential of the cloud come into even clearer focus.

IaaS, PaaS, and SaaS defined and sized

Let us now delve into some of the characteristics of cloud computing to understand the options open to companies considering how best to leverage the cloud for their IT needs. While cloud as a whole is a delivery mechanism for infrastructure and applications, there are different types of cloud services available, requiring different levels of expertise and involvement from the enterprises they serve. There are three widely used categories for discussing cloud services:

- **Infrastructure as a service** (**IaaS**), which delivers infrastructure components such as compute, network, storage, and virtualization as services
- **Platform as a service** (**PaaS**), which in addition to the IaaS layers, also provides an application development environment via an application programming interface (API) for developers to write to before they deploy their apps onto the platform
- **Software as a service** (**SaaS**), in which the entire application stack, including the application itself, is delivered as a service

Ease of adoption meant SaaS took off first and became the largest market

SaaS clearly makes the fewest demands on the enterprise customer, which can simply sign up and start using the service, with minimal configuration effort required beyond, in some cases, uploading its data into the provider's platform (e.g., in Salesforce).

This ease of adoption also made SaaS the early breakout star of cloud computing, and it remains a mainstay of the overall market. Omdia estimates that spending on SaaS services totaled $58bn in the first half of 2020, a 28% increase on the same period in 2019. If we extrapolate that growth rate through the end of the year (which seems reasonable given the uptick in demand for cloud services as a result of the coronavirus pandemic), the SaaS market will come in at around $125bn for 2020.

IaaS offers great rewards for more effort

At the other end of the spectrum, IaaS requires most effort from the enterprise customer, which becomes responsible for everything from the operating system (OS) on which the application will run, through the app itself, up to and including the data.

Therefore, it requires the involvement of more people within the customer's organization. If it is migrating an existing application from its own premises into the cloud, IT operations will need to be involved, and if it is writing a new app for the cloud, its developers will also need to get involved. IaaS adoption is therefore a weightier undertaking, requiring a higher degree of confidence on the part of an enterprise, and for this reason, its growth has been a more recent phenomenon as companies' comfort levels have risen.

That said, IaaS offers the enterprise customer considerably more control and freedom of movement than SaaS does, and for this reason it has now grown to be the largest segment of the market. Omdia estimates that it was worth $64bn in the first half of 2020 and extrapolates that to $138bn for the entire year.

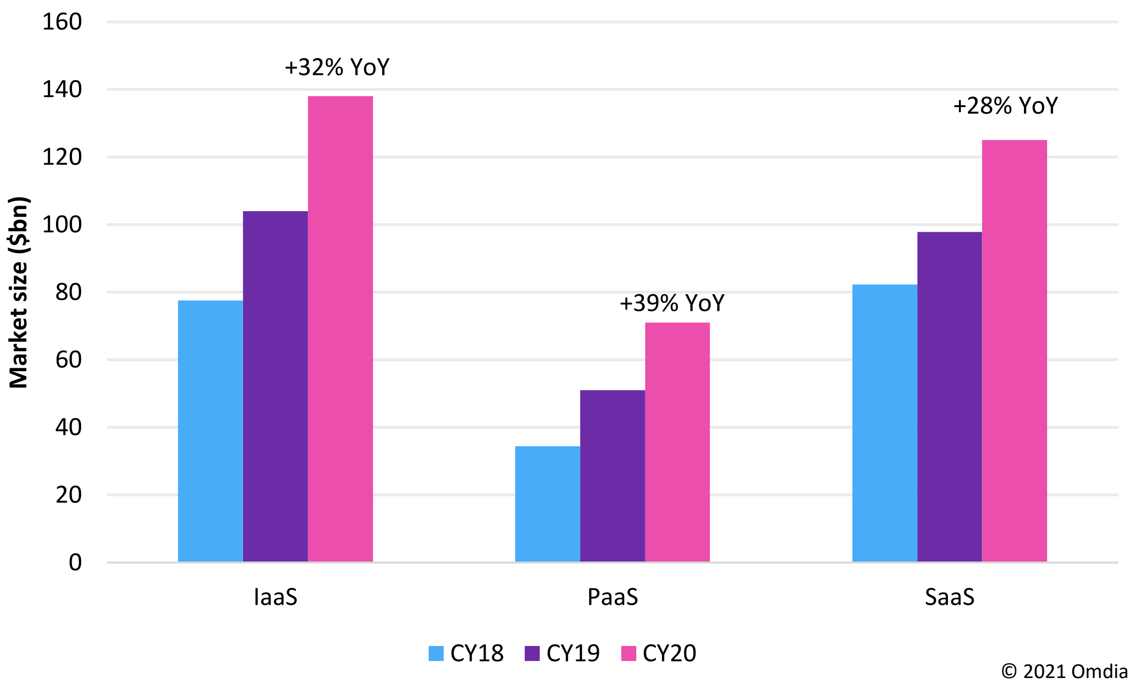
It is also worth pointing out that the greater barriers to entry for IaaS mean that it is not for every size or type of company, and the same is true for PaaS. You need more in-house expertise to be an IaaS or PaaS user. With SaaS you simply consume the end product, that is, the application.

PaaS is the fastest-growing segment of the cloud market

PaaS, meanwhile, can be thought of as a halfway house between the previous two modes of cloud delivery, affording more control over the application than SaaS but with less of the heavy lifting required for IaaS, because the cloud service provider (CSP) is responsible for the underlying runtime environment and OS.

Of course, this limits the "mobility" of the application: its owner cannot simply shift it from one CSP to another, having written it to a proprietary API, so there is an element of tie-in. That said, PaaS is clearly proving to be the most popular delivery mode for cloud computing of late, enjoying the fastest growth rate overall. Omdia's numbers for the first half of last year put the PaaS market at $32bn, which it extrapolates to $71bn for all of 2020. By this calculation, PaaS grew 39% in 2020, compared to IaaS's 32% and SaaS's 28%.

Figure 1: How the IaaS, PaaS, and SaaS markets are growing



Source: Omdia

A couple of observations here. First, the numbers for CY20 are estimates, because Omdia's Cloud and Data Center Practice has yet to publish its definitive numbers for the full year. The calculation was based on the first half of 2020, extrapolating on the assumption that the growth rate for 1H20 was identical to the growth rate for 2H20. Clearly this may not have been the case, particularly for SaaS, which enjoyed a veritable explosion last year because of the pandemic, so much so that the $125bn estimate may in fact understate the size of that market, coming in below the final published number.

Second, IaaS's overtaking SaaS as the largest segment in 2019 (SaaS was consistently the largest for every year prior to that) can be attributed to a couple of factors:

- An increasing number of companies have grown more comfortable with cloud and thus have also gotten more adventurous, dipping their toe into the more complex worlds of IaaS and PaaS.
- The advent and growth in popularity of containers, which can be thought of as the second generation of cloud infrastructure, coming after virtual machines, has led to a faster uptake of the more demanding delivery models for cloud computing. Docker was founded in 2010, and Google launched Kubernetes in 2015, so the recent growth in both IaaS and PaaS can be attributed, at least in part, to these more modern app architectures coming to maturity.

Private, public, hybrid, and multicloud

It is now worth mentioning a few other terms that are commonly used in discussing cloud computing. The first of these is a dichotomy, namely *private cloud* or *public cloud*. These two terms, both of which refer to IaaS and PaaS environments, are fairly intuitive:

- **Public cloud** is simply a service such as AWS's EC2 or S3, where the customer pays for the resource (in these cases, processors or storage capacity) in an environment where the instances it pays for will be located in a multi-tenanted environment alongside instances that are being used by other customers.

- **Private cloud** refers to the scenario where an enterprise has "cloudified" its data center infrastructure, enabling compute and storage capacity to be served up on demand to its internal users, flexing up and down dynamically rather than with preordained limitations set by the number of processors in a given server or the gigabytes of capacity in a particular RAID array. In a private cloud, the infrastructure still belongs to the customer and resides on its premises, but it achieves the flexible capacity benefits of the cloud.

However, between these two fairly obvious categories there is a third, namely *virtual private cloud* (VPC). Perceiving that the more security-conscious customers in regulated industries such as banking and insurance were loath to enter the public cloud for fear of their data being seen by other entities using the same infrastructure, the leading CSPs came up with a best-of-both-worlds offering. This is a service model whereby the customer pays a premium to get a fully dedicated cloud infrastructure that belongs to the CSP but is for the customer's exclusive use only. This makes it effectively private, even though it does not belong to the customer or reside on its premises.

The private/public dichotomy, and especially the advent of VPCs around 2010 (AWS launched its offering in 2009) led to the evolution of *hybrid cloud*, where a company keeps part of its infrastructure, applications, and data in a private cloud or VPC but has the other part in the public cloud. It may, for instance, keep its most sensitive customer data in the private realm but anonymize it for analytical purposes then run analytics on it in the public cloud.

Finally, there is *multicloud*, the situation in which an enterprise uses more than one CSP, often taking advantage of the strengths of each: AWS excels in the breadth and depth of its services, for instance, while Microsoft's dominance in office productivity makes it a favored destination for certain types of workload, and Google's strength in artificial intelligence (AI) gives it an edge for any analytical application leveraging AI. Such multicloud environments are also quite often hybrid, with at least some functionality still residing on the customer's premises.

It is also worth pointing out that the term *multicloud* is also frequently used to mean *multimode*, where an organization uses different providers, some for IaaS, some for SaaS, and potentially even one for PaaS. This actually took off earlier than a "multi-IaaS" scenario: many companies will use Salesforce for their customer relationship management (CRM) needs while getting their emails delivered by Office 365, and they may even be running their IT service management (ITSM) on ServiceNow. They are already "multi-SaaS," before they ever countenance using one or several IaaS or PaaS providers.

The benefits of cloud adoption for media and entertainment

So what are the benefits of moving to the cloud? Most of them are generic: they apply to any type of company, regardless of which vertical it is in, but there are also particular benefits for the media and entertainment (M&E) industry.

Infrastructure that flexes up and down

The most obvious benefit is in the increased flexibility of infrastructure. The notion of “spinning up” additional capacity of compute or storage, all of it with the requisite network connections, differs radically from the on-premises world in which servers or storage devices would need first to be provisioned by the enterprise, then installed and tested by IT, then loaded with the necessary applications to be commissioned for production, which could result in weeks or even months of delay. In contrast, cloud capacity is, at least notionally, infinite and, even more critically, available on demand.

This has implications for companies in M&E. The most obvious of these is the ability to become more events driven, responding to situations in a more short-term, “pop-up” manner than was previously possible. For instance, a company may assemble a team to promote, then broadcast to a global audience, a particular sporting event such as a boxing match once every quarter, standing up the necessary cloud infrastructure for this purpose then tearing it down straight afterward. Annual music or film festivals could be covered in this way, with capacity autoscaling to address sudden peaks in demand. Sotheby’s could do the same to auction a particularly sought-after artwork by an old master. In other words, pop-up broadcasting, at least of the streaming variety, becomes possible in a way that it was not before.

Capex becomes opex

There is also a cost benefit, though it would be wrong to suggest that cloud computing is necessarily cheaper than the on-premises alternative. The main impact of cloud is that what previously were capital expenditure costs (capex) become operating expenditure (opex), with the ability to go down when business activity slows, the classic example being seasonal sports such as English Premier League soccer, Indian Premier League cricket, and “hyper events” such as the Olympic Games and the Cricket World Cup, where there is a short-term requirement for huge amounts of bandwidth. And of course, in such scenarios, capacity can be spun down as well as up.

Faster iteration of application code

Then there is the benefit to your applications. We have already discussed how infrastructure provisioning is accelerated in the cloud, but the same goes for the apps themselves. It is not uncommon for online retailers to update their customer-facing applications several times a day: Netflix pushes new code several hundred times a day, while AWS’s e-tailer parent Amazon famously deploys code an average of 23,000 times every day. Even for private apps, that is, those that are only for use by a company’s own employees, the ability to iterate more frequently means multiple changes can be introduced on a daily basis.

The Agile development approach and its concomitant impact on operations (the so-called DevOps trend) have contributed to this process. Most recently, the need to innovate rapidly on the web has been turbocharged by the changes to working practices wrought by the pandemic, which drove entire populations into online commerce.

This is certainly also the case for M&E, where there is a need for video services and gaming platforms to adapt to consumer tastes and requirements and to changing consumption patterns: demand is no longer concentrated in the evenings, for instance, nor even particularly predictable. Providers need to respond, in near-real time, with faster integration of new and additional content.

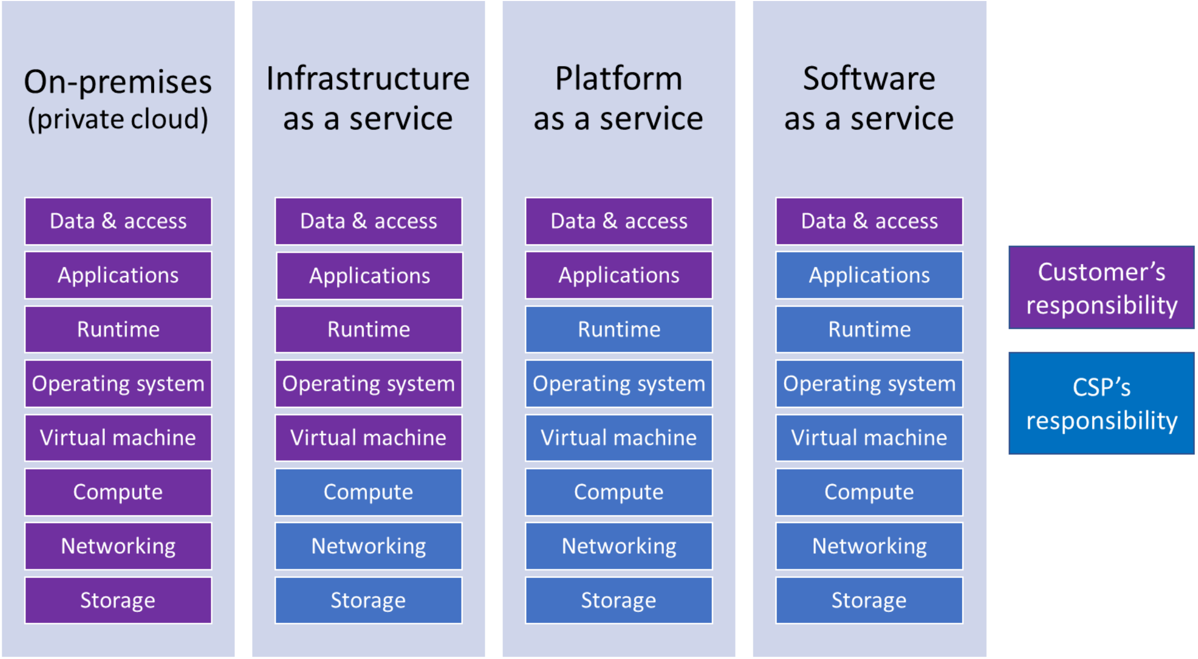
Greater collection of threat data and faster remedial action

While we will focus on security later in this document, it is worth mentioning here that cloud computing brings one clear benefit for security professionals. Threat data can be collected from across a cloud estate and sent to a common backend repository (typically a data lake) for analysis, after which remedial actions can be pushed out to the relevant systems such as virtual firewalls, micro-segmentation systems, and cloud workload protection platforms. The process can be far more dynamic than in the old world of analyzing logs in a security information and event management (SIEM) system then opening a ticket in an ITSM platform.

Cloud security

Now we come to the crucial topic of cloud security. How secure is the cloud? How much can you expect from your CSP, and how much is your responsibility? At this point, it is worth introducing the concept of the shared responsibility model for cloud security.

Figure 2: The shared responsibility model for cloud security



On-premises (private cloud)	Infrastructure as a service	Platform as a service	Software as a service
🟪 Data & access	🟪 Data & access	🟪 Data & access	🟪 Data & access
🟪 Applications	🟪 Applications	🟪 Applications	🟦 Applications
🟪 Runtime	🟪 Runtime	🟦 Runtime	🟦 Runtime
🟪 Operating system	🟪 Operating system	🟦 Operating system	🟦 Operating system
🟪 Virtual machine	🟪 Virtual machine	🟦 Virtual machine	🟦 Virtual machine
🟪 Compute	🟦 Compute	🟦 Compute	🟦 Compute
🟪 Networking	🟦 Networking	🟦 Networking	🟦 Networking
🟪 Storage	🟦 Storage	🟦 Storage	🟦 Storage

🟪 Customer's responsibility

🟦 CSP's responsibility

© 2021 Omdia

Source: Omdia

The model makes clear which parts of the computing stack the CSP takes responsibility for (including their security) and which remain the responsibility of the customer. **Figure 2** dates from an era when all cloud computing relied on classic server virtualization technology, involving virtual machines (VMs). It is true that cloud has moved on since then with the introduction first of container technology and, even more recently, of serverless, and there are more advanced versions of the diagram that encompass those new compute paradigms. However, for our current purposes, this version will suffice.

Whereas in the on-premises world, the organization operating the infrastructure took complete responsibility for procuring, deploying, managing, and securing it, IaaS sees the CSP taking control of the bottom layers of the stack, and by the time we reach SaaS, the customer of the service must take responsibility only for the data on which computations will be made there and for the access rights of its employees and third parties such as business partners. Indeed, the one constant across all the types of cloud computing in the diagram is the fact that the customer is always responsible for data, and thus also the content, and who has access to it.

TV and video service providers are at the center of the connected app economy

Cloud is at the juncture of this transformation journey

In today's highly fragmented digital media arena, TV and video service providers are steadily focusing on building highly localized, tailored, and interactive direct-to-consumer (D2C) services such as over-the-top (OTT) video, not just to accelerate their market penetration but also to enhance their long-term competitive edge. D2C OTT video is a highly competitive market in which the ability to promote loyalty and retain customers is a differentiator.

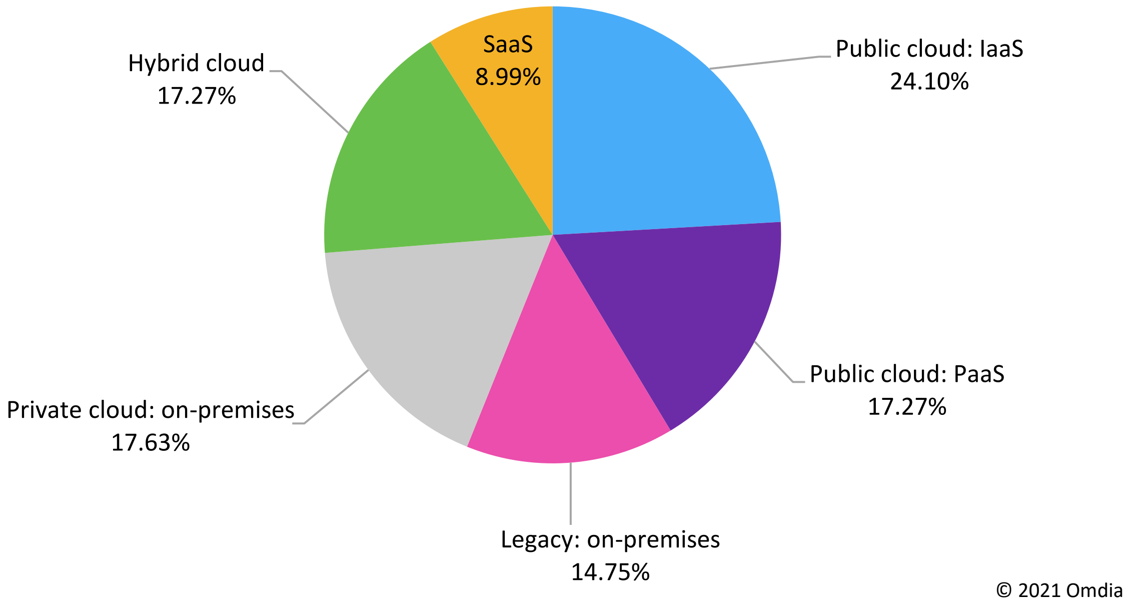
This has led to a majority of TV and video service providers embarking on a data-first strategy to deliver premium quality of engagement. Furthermore, as D2C has become the flagship engagement approach for TV and video content, applications of both the enterprise and consumer-facing variety are crucially important. Utilization of multiformat, layered, and dimensional application repositories requires a highly scalable and agile backbone, which has led to accelerated investments into cloud-based environments.

Traditionally, TV and video service providers have adopted a fairly conservative cloud migration strategy for fear of loss of control, doubling down instead on investments in legacy on-premises infrastructure and in-house services. But as business priorities move toward hybrid monetization, faster time to market, and operational productivity, the push to cloud is inevitable in the long run.

The movement of industry-specific applications to the cloud

Omdia's ICT Enterprise Insights (ICTEI) survey for 2020/21 highlighted that almost 18% of industry-specific applications—such as multiplatform engagement and enterprise apps such as media asset management (MAM), playout, and multiplatform—will be moved to hybrid cloud in 2021. Also noteworthy is the fact that almost a quarter of industry-specific applications will be on public cloud (the IaaS variety). SaaS is the smallest segment, though almost 9% will leverage it as the primary delivery strategy, thus confirming the evolution and acceleration of a hybrid multicloud delivery environment in the media space.

Figure 3: TV & video service providers' delivery strategy for industry-specific apps, 2021



Source: Omdia

Furthermore, launching new digital services to reduce churn is a key performance indicator (KPI) for most media enterprises globally. Of course, this needs to be done in a cost-effective manner, and with customer acquisition costs rising, the move to new-age infrastructure, with the concomitant shift from capex to opex, is essential for safeguarding profitability margins.

Since most M&E enterprises have invested heavily in on-premises infrastructure, writing off such investments will not be feasible in the short term. That being the case, the most likely scenario for the immediate future is the development of hybrid multicloud infrastructures, with some functionality remaining on the provider's premises while other parts move into the cloud, that is, some combination of public cloud/IaaS or PaaS, on-premises, and SaaS as depicted in **Figure 3**.

Each M&E segment has its own priorities for cloud adoption

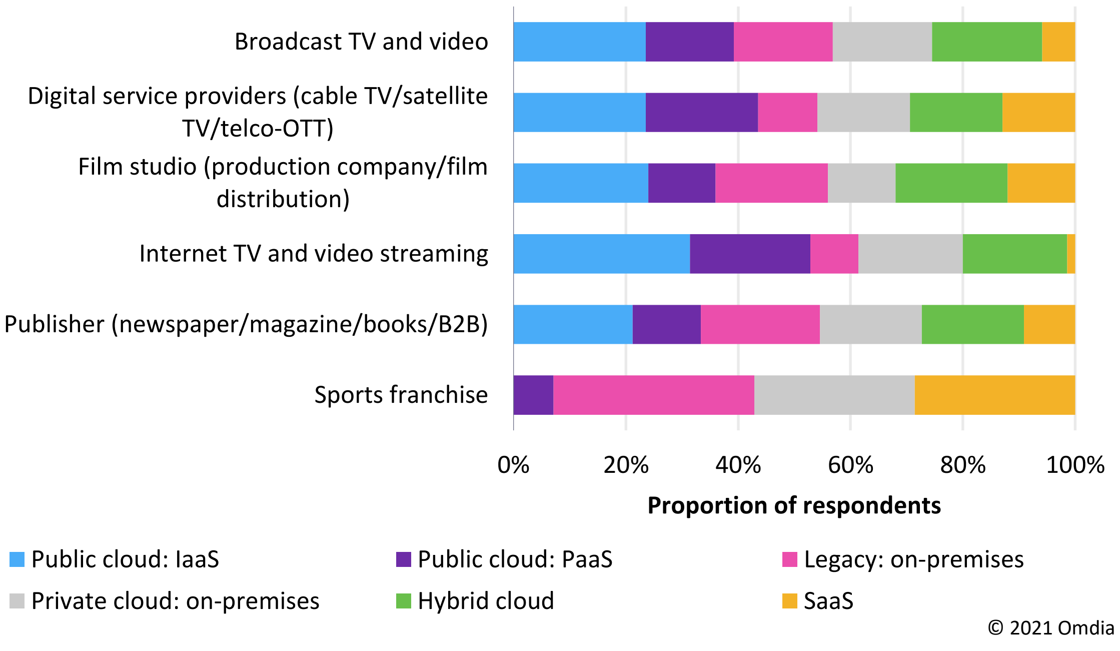
Omdia's ICTEI survey 2020/21 revealed that pure-play OTT video services such as Netflix and Amazon Prime will be pushing almost half their industry-specific applications to the public cloud. Compare this with sports franchises, which will keep almost a third of their industry-specific applications on legacy infrastructure (i.e., on-premises).

However, sports franchises will also be at the forefront of fully hosted SaaS delivery strategy for their industry-specific applications, with almost 29% of these workloads being pushed into this format. As time to market becomes the primary business priority for most sports franchises moving toward a

D2C services growth trajectory, leveraging a SaaS delivery strategy is imminent. Omdia's ICTEI survey 2020/21 showed that almost 23% of sports franchises will be launching their own D2C offerings in the next two to three years. In other words, each type of media enterprise will follow a different delivery route and dynamic, depending on their CXO/CIO culture, long-term business scenarios, priorities, and budgets.

Distributed infrastructure demands hyperscalable security

Figure 4: TV and video service providers' delivery strategy for industry-specific apps by segment, 2021–23



Source: Omdia

Figure 4 indicates that media enterprises will utilize a hybrid multicloud model in the coming years. Migration of enterprise and consumer applications along with their associated data (including the industry-specific variety) to a cloud backbone is a complex transformation journey, but the real obstacles are security risks.

Security requirements will vary across the different delivery models

It would be wrong to suggest that any of the six delivery models in **Figure 4** is inherently more secure than another. Rather, each presents its own type of risk. The on-premises private cloud variant, for instance, may look more secure because it is completely under the control of enterprise from the physical data center all the way up the stack to the data/content. However, if an enterprise suffers a supply chain breach along the lines of the now infamous SolarWinds attack made public in December 2020, being on-premises or in the cloud will make little difference, because resources in both those environments were compromised.

Equally, while the more security-conscious enterprises may favor a VPC over the public cloud (a VPC here being roughly equivalent to the "Public cloud: PaaS" category in **Figure 4**), there is scant evidence to suggest that one is noticeably more insecure than another. In many cases, the driver for the VPC option may in fact be compliance, that is, the ability to demonstrate that you have gone for the "most secure" cloud option.

What is also clear across the various delivery models is the difference in the level of responsibility for security that the enterprise customers will have vis-à-vis the CSPs. As the shared responsibility model demonstrates, in the "Public cloud: IaaS" model, the enterprise must take responsibility for securing everything from the VM upward, whereas at the other end of the spectrum, in the SaaS model, its responsibility will be limited to the data/content itself, with the CSP providing security for all the layers below that in the stack.

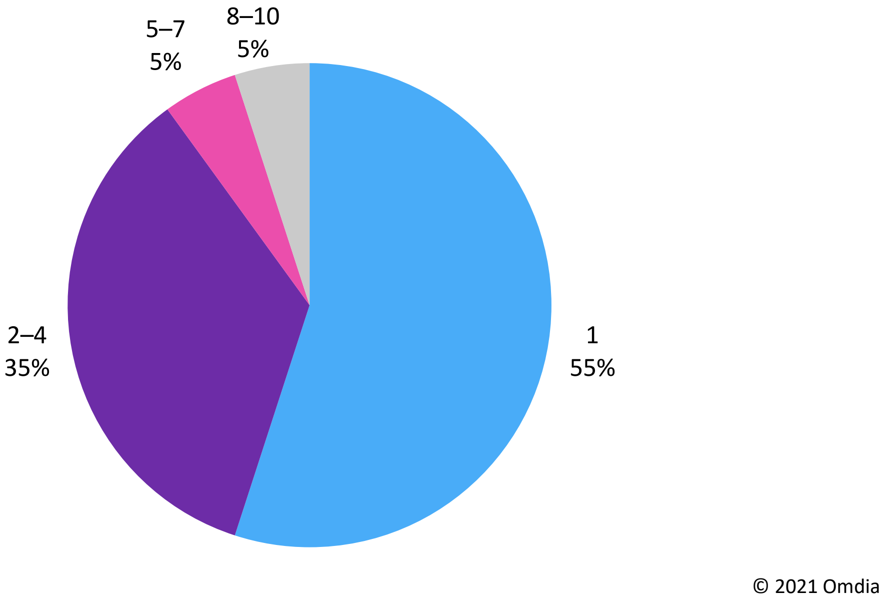
Scalable enterprisewide security will be key

As the hybrid multicloud approach to delivery that emerges from **Figure 4** becomes the norm across the M&E sector in the coming years, enterprises adopting this strategy will need to deploy security tools that can not only scale during times of peak activity but ideally also span the different cloud and on-premises environments that make up the customer's hybrid infrastructure. This will be fundamental if a company is to gain an enterprisewide view of its attack surface and take remedial action across its infrastructure.

Security, and especially content protection (both before and after launch), has been at the center of media enterprises' business priorities for decades. Omdia's ICTEI survey 2020/21 highlighted that end-to-end premium content protection is one of the top three business priorities for 37% of media enterprises globally in the next 18–24 months. Almost the same proportion (34%) stated that application security is fast becoming one of their key investment areas over the next two to three years.

Furthermore, as spend on cloud-based infrastructure surges across most M&E segments, the security of applications, content, and data will be crucial to enhance sustainable competitive advantage. Therefore, there will be a need for media enterprises to turn to long-tail strategic vendors offering a strong value proposition across not just content but also application and infrastructure. Omdia conducted a survey with nearly 40 media enterprises to understand the vendor configuration they prefer across their end-to-end security ecosystem. More than half (55%) said they prefer a single vendor to handle their security requirements.

Figure 5: How many vendors do you plan to use for your end-to-end security (content, apps, infrastructure)?



Source: Omdia

An evolutionary model for cloud security

We have surveyed the three main delivery modes for cloud computing and seen how the shared responsibility model for cloud security allocates different levels of customer responsibility across each of them. We have also discussed the desirability, from an investment perspective, of hybrid multicloud infrastructures in the context of the M&E sector. Now let us look at how a company in this sector that wants to adopt some form of cloud computing should think about security. M&E security specialist Verimatrix recommends a layered approach to ensure any gaps are covered.

The baseline: Native cloud security

All CSPs offer some level of security capability for you to use their services. This will include securing the physical data center in which they are located and guaranteeing a continuous supply of power and water but also making load balancers available for your traffic and imposing controls over how and by whom your machine instances are accessed. Many CSPs operate an identity and access management platform for this purpose, while most of the big ones will also offer encryption key management as a service for your data. Make sure you take full advantage.

Extended cloud security

This is where you need to think about bringing in third-party security providers to supplement what the CSP itself is offering. The capabilities include endpoint protection, subscriber and entitlement management platforms, and delivery of edge-based, just-in-time services that enable a secure connection between the encoders and your content delivery network (CDN) provider.

Technology that enables the secure exchange of credentials is a key capability here, as are monitoring traffic between the encoders and encryptors, and data security both for the consumer and the operator.

Reactive cloud security

The security techniques in this category are designed to let you know whether (1) any of the code you are developing would introduce vulnerabilities into your infrastructure that could be exploited by an attacker and (2) your infrastructure is actually being probed with a view to finding such vulnerabilities. Vulnerability-scanning technology has a key role to play for the preventive dimension, while intrusion-detection systems can provide the runtime protection of the code you already have in production.

Conclusion

Recommendations

Cloud computing has gone mainstream, so get up to speed with it

Cloud computing is a more flexible, responsive, and scalable way of delivering IT and has reached a level of maturity that means you should get to know how it works, what the options are for adopting it, and what the pros and cons are of the various approaches to deploying and using it. SaaS was the first segment to take off and has the lowest barriers to entry. The IaaS and PaaS markets developed more recently, primarily because they demand more of the organization adopting them. Indeed, it is fair to say that they are not for every size or type of organization: it will depend on a number of factors, including your company size and available resources, your business goals and strategy, and your level of commitment to application development.

Adopt hybrid multicloud to enable OTT monetization and faster time to market

Unification of the content supply chain, hybrid D2C monetization avenues, and time to market remain the core business priorities, effectively mandating an aggressive push toward cloud-based infrastructure and services. However, the majority of media enterprises have traditionally built in-house capabilities via a steady stream of investment into on-premises platforms, so writing off these investments is challenging in the short term. Nonetheless, a move to a hybrid multicloud environment is inevitable in the long run.

Understand the implications of the shared responsibility model for cloud security

Familiarize yourself with the model, how each of the delivery modes for cloud computing has differing implications in terms of what you will be responsible for, and how your responsibilities will change as your infrastructure transitions between them. Bear in mind that this process may not be linear: for some requirements you may go straight to SaaS and thus retain responsibility only for securing the data. In other cases, you may move an app into or develop it specifically for an IaaS or PaaS environment, with the concomitant additional security responsibilities, but after a time discover that you can change it to SaaS.

Select a single strategic partner for security

The migration of workflows to the cloud will vary across the content supply chain, depending on primary and secondary business priorities and on annual IT budgets. However this migration happens, this “cloudification” of infrastructure in the M&E sector will demand heightened security for both enterprise and consumer-facing applications in this highly fragmented ecosystem. Choosing a single, end-to-end strategic partner for security is recommended as a means of reducing revenue leakage and enhancing competitive edge. Consider your partner’s agility in adapting to your evolving cloud requirements.

Appendix

Methodology

Omdia has leveraged multiple internal resources for creating this thought leadership piece. The database used include

Annual ICTEI survey encompassing ICT spend trends across all the media technology stacks within nine submedia and entertainment industries with an interview sample of 344 enterprises globally.

Enterprise spend forecast on cloud services: this is Omdia’s flagship spend forecast across all the three cloud services subverticals globally

Authors

Rik Turner
Principal Analyst, Cybersecurity
customersuccess@omdia.com

Kedar Mohite
Principal Consultant, Media Technology
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About Verimatrix

Verimatrix (Euronext Paris: VMX) helps power the modern connected world with security made for people. It protects digital content, applications, and devices with intuitive, people-centered, and frictionless security. Leading brands turn to Verimatrix to secure content including premium movies and live-streaming sports, sensitive financial and healthcare data, and mission-critical mobile applications. It enables the trusted connections its customers depend on to deliver compelling content and experiences to millions of consumers around the world. Verimatrix helps partners get to market faster, scale easily, protect valuable revenue streams, and win new business.

www.verimatrix.com/products/multi-drm

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.