iamt

connect | support | inform

# Megatrends

## Security in MediaTech Ecosystems

Business Intelligence Unit, IABM, August 2025

18 April 2026

# *Table of contents*



# About this report

**Connect. Support. Inform.**
theiabm.org

# *Megatrends research family*

## IABM's Megatrends research examines selected industry topics

Megatrends research explores transformative shifts in MediaTech. In 2025, we are investigating three key trends, based on our ongoing research and discussions with our valued members and Global Engaged Partners (GEPs): Business Transformation, Security in MediaTech Ecosystems, and Game Industry Convergence. This report focuses on our research findings about Security in MediaTech Ecosystems.

### Business Transformation

Focus on strategies for successful business transformation in MediaTech.

### Security in MediaTech Ecosystems

Focus on strategies for strengthening security infrastructure, enhancing content protection, and mitigating AI-related vulnerabilities in an increasingly digital ecosystem.

### Game Industry Convergence

Focus on strategies for IP monetization, viewer engagement through fan communities and interactivity as well as production synergies (e.g. virtual production, game engine, VFX).

Source: IABM

# Research Methodology

## This report was prepared using a hybrid research approach

This report leverages a comprehensive, hybrid research approach, combining diverse data sources and methodologies to ensure a holistic view of the industry trends. Our methodology encompasses the following key components:

### Primary Research

**Quantitative:** Survey data is at the core of our analysis, providing quantitative insights into the indust prevailing trends and sentiments.

**Qualitative:** To complement our quantitative data, we conducted in-depth interviews with a select gr industry experts. These discussions have provided rich qualitative insights, adding depth and context to findings.

### Secondary Research

**Desk-based:** Our research is further enhanced by an extensive review of both structured and unstruct public data. This includes an analysis of industry executive quotes, reports, and publications, which offe valuable perspectives on industry trends.

We have also incorporated quantitative data from reputable external sources. This data has been carefu selected to enrich our understanding of the industry dynamics and to provide a benchmark against our p research findings.

# This report includes an executive summary and the main body

- The first section of this report provides a brief overview of key insights from the main report and can be read as an executive summary.
- The main body of this report provides a detailed analysis of security trends in MediaTech ecosystems, investment patterns, and strategic approaches to counter evolving cyber threats and maintain audience trust.

All sources used in this report are reported at the bottom of each slide. Some slides include a brief explanation of the data manipulation steps we adopted to better illustrate industry trends.

If you have any feedback about this report, please contact us at insight@theiabm.org.
We would really appreciate it, as we always strive to improve our research.

# Snap Insights

**Connect. Support. Inform.**
theiabm.org

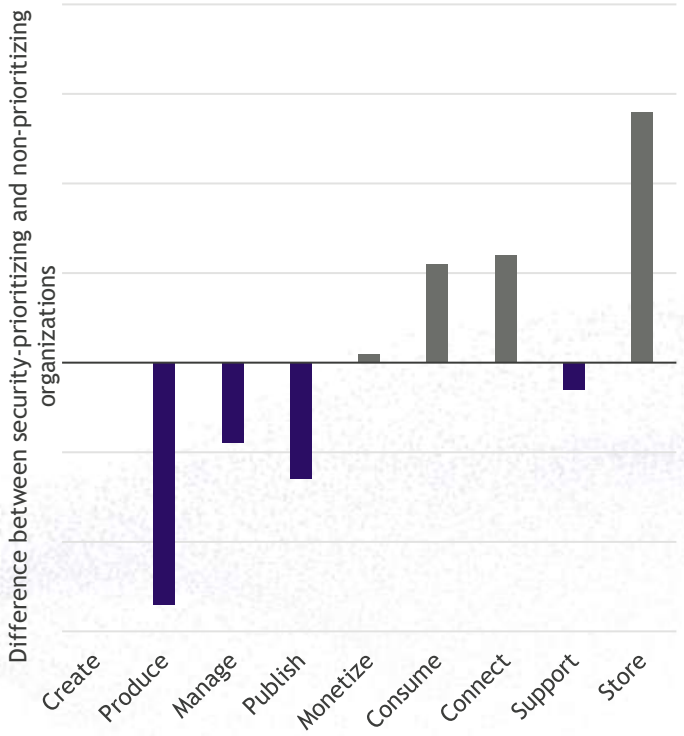
# Snap Insights

## Security has become the second fastest-growing trend in industry technology roadmaps

### Investment in security is growing

IABM data shows the growing importance of security (including cyber, encryption, and conditional access) in the broadcast and media industry's technology roadmaps. Security has risen by 5 percentage points year-over-over in 2025 and became the second fastest-growing trend, following artificial intelligence (AI) and machine learning (ML).

Companies that prioritize security are focusing on the consume, connect and store segments of the content supply chain




Q. Which of the following content supply chain segments are relevant to your organization? (Feb-Jun 2025, n=241)

## Drivers of change

### Transition to OTT and streaming

As traditional broadcast and media companies are changing their distribution models to OTT (over-the-top) content delivery, security investment shifts towards latter stages of the content supply chain. The highly fragmented streaming landscape and the vulnerability of streaming devices expands the attack surface due to the majority of audiences consuming content on open devices, where various third-party software can be installed.

### Transition to cloud and and IP-based workflows

As media companies transition to software-defined workflows, they are expanding their network perimeter and significantly increasing their risk surface. This evolution has shifted investment priorities from solely protecting content to securing infrastructure and entire workflows.

Source: IABM

Snap Insights

# Transition to software-defined workflows and proliferation of AI pose new security threats

## Securing Infrastructure

### The shift toward Zero Trust security

Zero Trust principles remain in the early stage of adoption in the M&E industry, though there is a clear upward trend in investment directed toward Zero Trust architecture.

### Human-related vulnerabilities

A lot of leaks or security issues are human-related and happen either due to malicious intentions of employees or due to neglecting certain principles. MediaTech suppliers are increasingly focusing on least-privilege access to ensure that only authorized users have access to their devices and are granted the minimum level of access required to perform their tasks. Continuous staff training is gaining importance to address new kinds of security threats, including AI-powered cyber attacks.

| Internal threats | External threats |
| --- | --- |
| Malicious intentions of employees, and neglecting best practice | AI-generated and AI-enhanced phishing attacks |

Source: IABM

## Protecting Content

### Growing piracy concerns

Pirates are increasingly targeting streaming platforms to steal content from live channels and build profitable business models using that content. Pirated streams are being redistributed via various social networks, multiplying the damage to broadcasters' and rights holders' revenues. A large share of investment in content protection remains within conditional access (CAS) but investment in this area is drastically declining in favor of multi-DRM (digital rights management) and watermarking solutions.

### Provenance and Authenticity

The growing adoption of AI poses significant risks, such as infringement of copyright and intellectual property, driving investment in verifying content provenance and authenticity and combating misinformation. Content authenticity is crucial for retaining viewership and maintaining audience trust. IABM's data shows the rise of investment in provenance and authenticity.

# Snap Insights

## Zero trust principles, training, and collaboration are key to addressing cyber threats

### Strategies to address cyber threats

**Strengthening perimeter (Zero Trust architecture)**

**Training employees**

**Fostering collaboration**

### AI in addressing security threats

The growing adoption of AI creates new kinds of threats, such as altering content, automating and scaling phishing and cyber attacks, impersonating individuals through deepfakes, and bypassing traditional security measures with adaptive behavior. However, AI is also increasingly used to protect both content and infrastructure in the broadcast and media industry.

MediaTech suppliers employ AI for behavioral analytics to identify unusual requests, which leads to cease-and-desist orders being issued to illicit streamers and the shutdown of illegal streams.

AI offers powerful capabilities to enhance content protection and infrastructure security, such as automated threat detection, anomaly identification, and real-time incident response

# Snap Insights

## Industry collaboration is essential for advancing security in the MediaTech ecosystem

### Future Outlook

### Securing software-defined media workflows

A recent development introduced by the European Broadcasting Union (EBU) – the Dynamic Media Facility (DMF) – demonstrates potential to facilitate secure software-defined media workflows. This development addresses critical security challenges stemming from expanding attack surfaces, increasingly complex security management, and the introduction of multi-tenant sharing. DMF defines a layered, modular model that enables interoperable broadcast and media workflows by combining strict design principles, modern encryption practices, and layered authentication mechanisms. Multi-tenancy isolation enables secure collaboration, so that different teams can operate within the same infrastructure without compromising each other's content or production workflows. The transition from proprietary frameworks to the Linux Foundation's open-source solution Media eXchange Layer (MXL) released in June 2025 accelerates the adoption of DMF.

### Ensuring audience trust

Investment in provenance and content authentication tools is expected to continue growing over the next two to three years. Media companies are likely to invest in internal systems that would validate signatures on content. The focus seems poised to shift from device to identity verification (from technical to editorial provenance) to ensure that content comes from trusted partners. Development of provenance tools requires a holistic approach and collaboration between CDN companies, security organizations, cloud service providers and industry bodies.

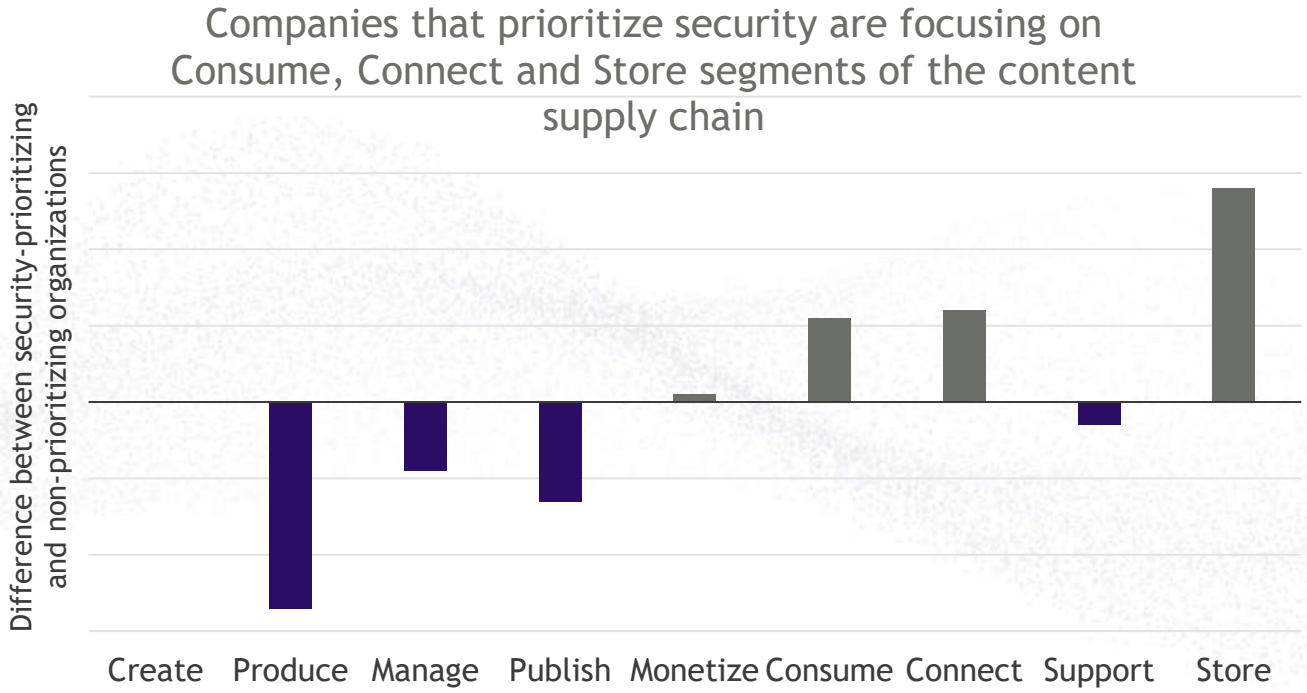
# Security Infrastructure in MediaTech Ecosystems

**Connect. Support. Inform.**
theiabm.org

# Security Investment

## Security investment shifts toward the latter stages of the content supply chain

The highly fragmented streaming landscape and the vulnerability of streaming devices is shifting security investment to the latter stages of the content supply chain. The attack surface is now much larger due to software-defined workflows and the fact that the majority of audiences are consuming content on open devices, where various third-party software can be installed.




MediaTech Supplier in an IABM interview

*This is not to say that content owners and production companies don't need to be careful about it - they definitely need to be careful in having the right measures in place - but if you see most of the piracy is happening downstream from that, really on the distribution side. I would say, 99.9% of the effort should be on the distribution side. That's really where most of the issues are happening.*

Rodrigo Fernandes
Product Director Content Security
Irdeto
(June 2025)

*The latest wave IABM's MediaTech Industry Tracker survey was conducted in February-March 2025, N=150

Source: IABM

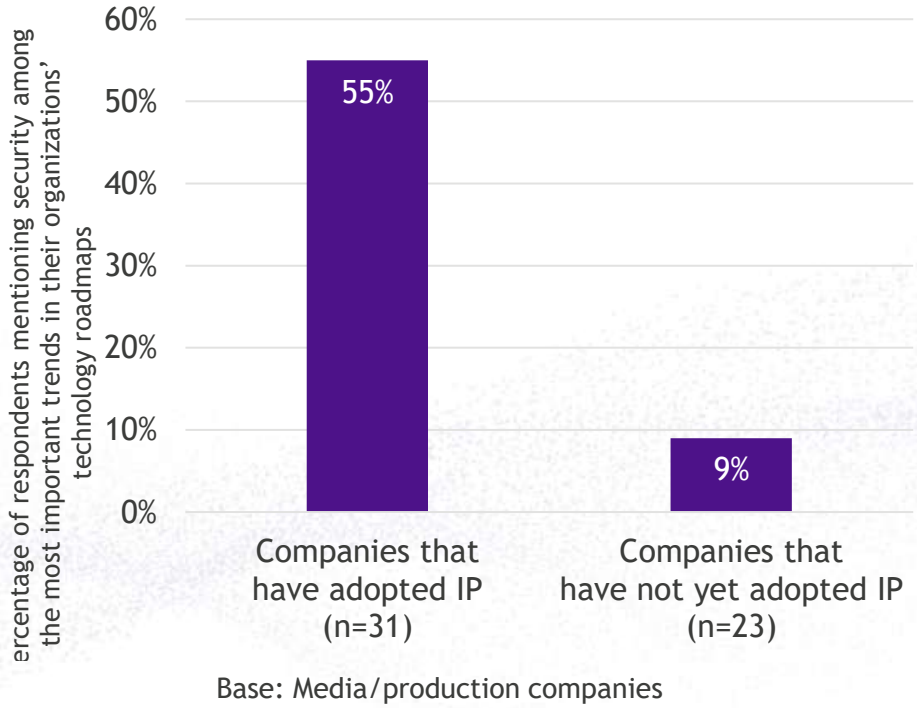
 

# Security Investment

## Transition from baseband to IP-based workflows and cloud environments

- The growing importance of security in the broadcast and media industry's technology roadmaps is primarily driven by the transition from traditional baseband infrastructures to cloud and IP-based workflows. In traditional baseband systems like SDI, infrastructure was relatively secure, as the predominant use of proprietary hardware resulted in very limited requirements for external network connectivity. However, with the shift to pure cloud and hybrid cloud models, media companies are expanding their network perimeter, significantly increasing the risk surface.
- IABM data shows that media and production companies adopting IP transport and networking (e.g., SMPTE ST 2110 standards suite) place greater emphasis on security in their technology roadmaps. The latest IABM data shows that cybersecurity ranked among the top 15 percentile of investment areas across the entire content supply chain and emerged as the leading investment area in content support, primarily driven by AI and cloud adoption. Most end-users expressed a preference for multiple cloud service providers for cloud computing, highlighting the increasing complexity of modern media infrastructures. The complexity of multi-cloud and hybrid cloud environments is exacerbating cyberthreats, driving the shift from reactive to proactive security strategies.

### Importance of security in organization's technology roadmap




Base: Media/production companies

*The latest wave IABM's MediaTech Industry Tracker survey was conducted in February-March 2025, N=150

Source: IABM

# Securing Infrastructure

## Vulnerabilities of IP-based systems and software-defined workflows

Migration to IP-based systems, cloud and software-defined workflows introduced new vulnerabilities. Key areas of concern include increased reliance on precise network timing, integration challenges with legacy technology, evolving AI-related phishing threats, and heightened risk of malware from external content sources.

### Reliance on PTP

Precision Time Protocol (standardized as IEEE 1588), which is an integral part of IP-based workflows, especially in live IP production, drastically improves synchronization precision in media workflows but introduces security limitations, such as a lack of built-in security, making it vulnerable to a range of security attacks such as delay attacks, message manipulation, spoofing, and unauthorized timestamp alteration. Tightening security controls on PTP systems creates trade-offs that can reduce timing precision, forcing system designers to weigh the need for maximal precision against the need for robust, scalable security strategies.

### Legacy Equipment and Files

**Legacy equipment**
Many legacy architectures were designed when security was not a priority, making them vulnerable when integrated with IP networks.

**Legacy files**
Archived media often contain dormant threats due to outdated detection tools. Archived content is rarely re-scanned after its initial storage. Old content received from external sources may contain malware designed to evade past scanning methods.

### AI-Powered Phishing Attacks

AI models now enable the creation of sophisticated, hyper-realistic phishing schemes that closely mimic legitimate communication, increasing human-related security vulnerabilities. While human-created phishing attacks still dominate the cyber threat landscape, AI-generated phishing attacks represent a rapidly evolving threat. These campaigns can be automated and scaled, overwhelming traditional detection and response systems. The emergence of AI-enhanced phishing attacks is driving the growing importance of training employees to identify these new types of threats.

### Ingest Workflows

The expansion of file transfer and content upload workflows in cloud-based and IP systems heightens the risk of malware and increases exposure to malicious scripts during content ingest. In their 2025 Data Breach Investigations Report, Verizon estimated that 30% of breaches were linked to third-party involvement – double the rate reported in the previous year. User-generated content (UGC) creates a large attack surface for malicious activity, leading to additional security risks.

Sources: IABM, SMPTE, Verizon, Hoxhunt

# Securing Infrastructure

## Strategies to address cyber threats

Key strategies to address new threats posed by migration to IP and cloud-based workflows include strengthening perimeter defences, training employees and tightening collaboration across the broadcast and media industry.

| | |
|---|---|
| **Strengthening Perimeter** | Strengthening perimeter includes hardening network infrastructure, introducing authentication systems, and deploying endpoint protection systems to prevent unauthorized access and mitigate potential threats. The cost associated with security tools and logging can be substantial, but this investment is justified by savings on recovery from security incidents, which is far greater. IBM's Cost of Data Breach Report 2024 estimated the global average cost of a data breach at 4.88m USD – a 10% increase from 2023. |
| **Training Employees** | AI-enhanced phishing attacks are becoming increasingly sophisticated, elevating the risk of human error. This necessitates effective employee training to help staff identify and effectively respond to these evolving threats. |
| **Fostering Collaboration** | Research participants highlighted the importance of industry collaboration facilitated by industry bodies to mitigate security risks.<br>• In the EU, the Cyber Resiliency Act mandates vendors to do coordinated vulnerability disclosure via European Union Agency for Cybersecurity (ENISA) who can manage the disclosure and provide unique identifiers to vulnerabilities.<br>• In the US, the government previously operated a range of structured and secure channels that enabled information sharing about cybersecurity threats between government organizations and private companies, including broadcasters. These channels include Information Sharing and Analysis Centers (ISACs), The Cybersecurity Information Sharing Act of 2015 (CISA 2015), and other federal programs and partnerships. However, in 2025, major policy and funding decisions significantly impacted these information-sharing structures, resulting in reduced funding and deprecated secure channels. |

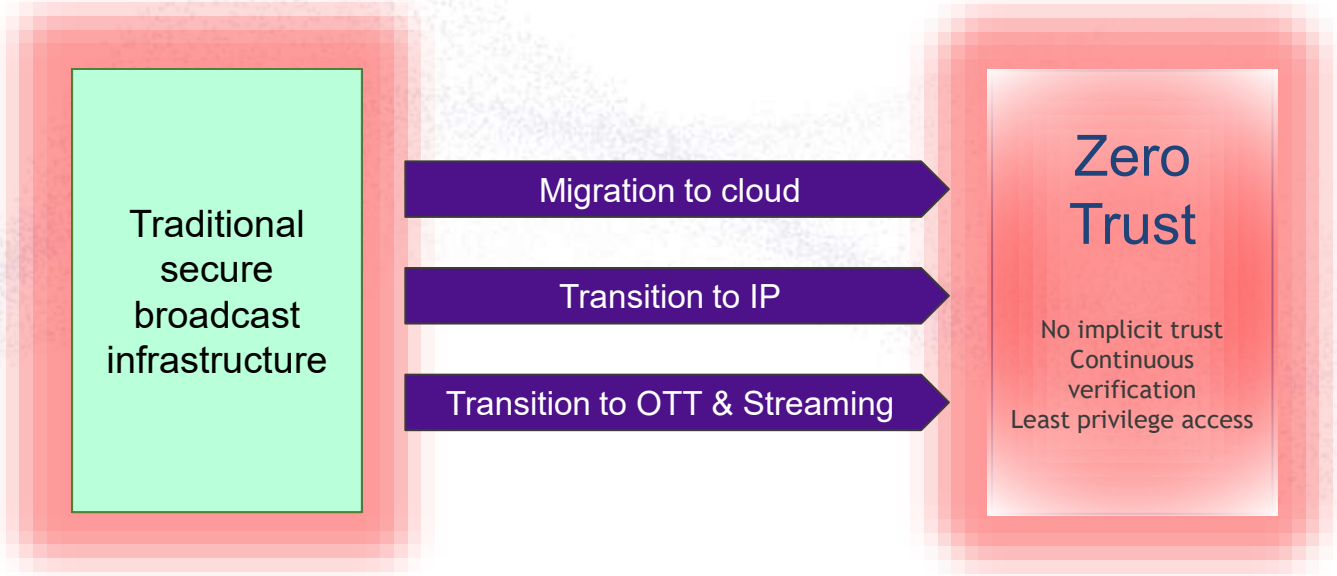
Sources: IABM, IBM

# Securing Infrastructure

## Digital transformation: Zero-trust security model

Due to digital transformation in the broadcast and media industry, the traditional security framework, which treats everything outside the facility and any outside actors gaining access to the network as a threat, has evolved into the zero-trust security model. This implies that everything inside or outside of the network is a potential threat, including human errors, misconfigurations of cloud environments, internal and external malicious actors, etc.




MediaTech Supplier in an IABM interview

*In the past, when distribution of content was within a facility or within a secure environment,* ***there was an implied assumption that you're within a secure environment.*** *Your networks are secure. Your machines are secure. The people in it are trusted, so you have to only focus on how to encrypt the content on one end and take it out on the other end.* ***Now, with these very complex workflows that go from facility to facility****, often bouncing over cloud, and in a B2B model from the cloud to many end users,* ***the assumption that you're in a secure environment goes away.***

Sergio Ammirata
Chief Scientist
Sip Radius
(June 2025)

SipRadius

Source: IABM

# Securing Infrastructure

## Digital transformation: Zero trust security model

In traditional linear content delivery and broadcast-specific infrastructure, content encryption was the primary security concern. However, the ongoing transition to increasingly complex digital ecosystems requires media companies to secure their entire workflows, including components such as workstations, routers, cloud relays, operating systems, and networks. The deeper security approach is necessary because in digital environments, malicious actors have no time limit to compromise security rather than only real-time opportunities when directly accessing physical environments.

A lot of leaks or security issues are human-related and happen either due to malicious intentions of employees or due to neglecting certain principles. MediaTech suppliers are increasingly focusing on least-privilege access to ensure that only authorized users have access to their devices and are granted the minimum level of access required to perform their tasks.

The growing sophistication of AI-generated phishing attacks requires enhanced education and training for staff to recognize and respond to these threats effectively.

# Securing Infrastructure

## Dynamic Media Facility

A recent development introduced by the European Broadcasting Union (EBU) to facilitate secure software-defined media workflows is the Dynamic Media Facility (DMF) – a comprehensive architecture for modern media production. It defines a layered, modular model that enables interoperable broadcast and media workflows by combining strict design principles, modern encryption practices, and layered authentication and authorization mechanisms. DMF embeds security throughout all its architectural layers – from physical infrastructure to media applications. DMF is underpinned by MXL (Media eXchange Layer) – an open-source software released in June 2025.

Provisioning | Control & Monitoring | Security

| | |
|---|---|
| Infrastructure | MXL infrastructure follows zero trust principles, including least privilege access, continuous monitoring and validation, device access control, and network segmentation. |
| Host Platform | Host platform prepares physical resources for containerization and are kept up to date through automated vulnerability patches application. Access to hosts and network switches is restricted according to zero trust principles. |
| Container Platform | Container platform orchestrates containers and media functions, with Kubernetes security best practices applied. |
| Media Exchange | Media exchange allows for high-performance data sharing between media functions through Remote Direct Memory Access (RDMA). Exchange between containers is tightly controlled through network policies and runtime security. |
| Media Functions | All control traffic is encrypted, using an open approach, at least as secure as TLS 1.3. All control clients are authorised using an approach at least as secure as OAuth2/JWT. |
| Applications & UI | Multi-tenancy approach ensures that multiple media organizations can use the same facility infrastructure securely and each tenant's UI/application context is strictly isolated so that no user can see or access another tenant's data or workflows. |

**September 3, 2024**
EBU published the foundational DMF Reference Architecture, establishing a layered, modular approach for software-defined media infrastructures

**April 4, 2025**
EBU in collaboration with the Linux Foundation and NABA announced the intent to form the MXL project.

**June 18, 2025**
The open-source software MXL SDK officially released to facilitate live media exchange on local or hosted compute infrastructure.

Sources: IABM, EBU, The Linux Foundation

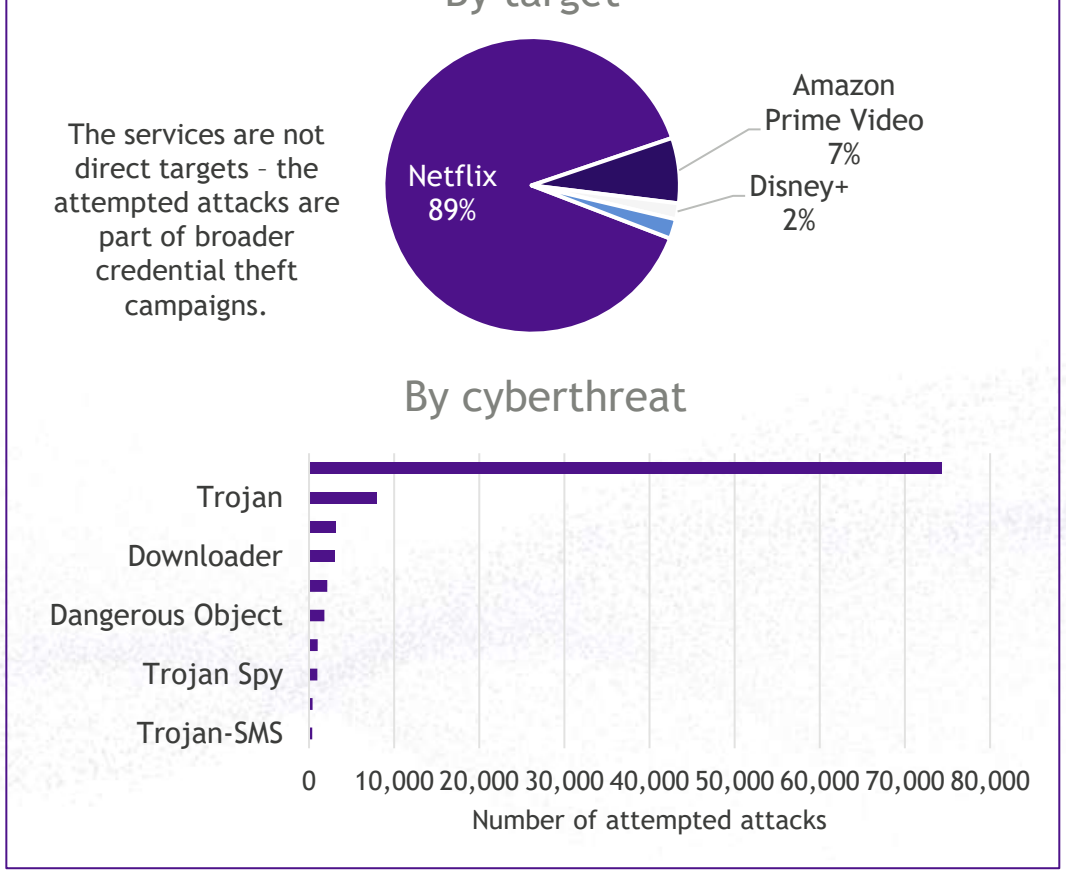
 

# Securing Infrastructure

## Cyberattacks on streaming platforms for credential theft

- Due to the popularity of streaming services, they are increasingly becoming targets for cybercriminals as part of broader credential theft campaigns. Based on anonymized threat statistics from Kaspersky Security Network (KSN), the company's Digital Footprint Intelligence team detected 96,288 attempted attacks disguised as the names of five major streaming platforms: Netflix, Amazon Prime Video, Disney+, Apple TV Plus and HBO Max from April 2024 to March 2025. The analysis revealed more than 7 million detected leaked accounts for streaming services in 2024.
- Within increasingly complex cloud environments, the number of cyber threats is growing along with false-positive alerts. With the rapid adoption of AI, ML, and deep learning, incident response tactics have evolved from a reactive response approach to proactive predictive threat mitigation. AI is helping address this issue by automating the prioritization of cyber threats and eliminating false-positive alerts, allowing cybersecurity teams to focus on high-risk threats.

### Attack attempts targeting major streaming platforms




Sources: IABM, Kaspersky

# Enhancing Content Protection

**Connect. Support. Inform.**
theiabm.org

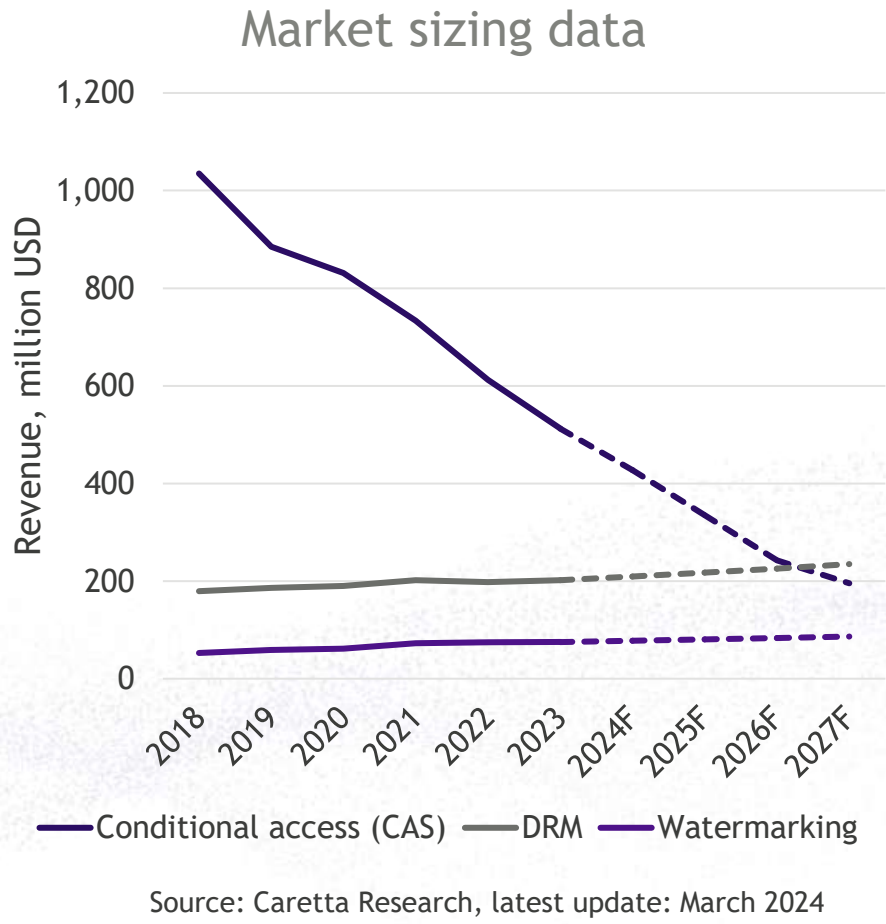
# Content protection: investment shifts from CAS to DRM and watermarking

A large share of investment in content protection is still within conditional access (CAS), which is fundamental for traditional broadcasters. However, with the industry's transition to increasingly complex and fragmented digital ecosystems, investment in this area is drastically declining in favor of multi-DRM and watermarking. Based on IABM's latest data, digital distribution (e.g., web, OTT, social media) is currently the top investment area by broadcasters and media companies. DRM and watermarking solutions are gaining importance due to growing piracy and the proliferation of AI.

MediaTech Supplier in an IABM interview

*For broadcasters, OTT business several years ago was still a side business. Now, they know this is the business. It means that they will at some point of time stop the broadcast over terrestrial and they will go full OTT. There are more and more requests on that.*

Pierre-Alexandre Bidard
EVP Products & Services
Viaccess-Orca
(June 2025)




Source: Caretta Research, latest update: March 2024

Sources: IABM, Caretta Research

# Content Protection

## The scale of streaming piracy

- Piracy continues to be a growing concern, particularly for OTT players, resulting in significant revenue losses for content owners and rights holders.
    - In India, streaming is the largest source of pirated content – it is estimated that streaming services lose up to 25% of their annual revenue due to piracy.
    - In the Middle East, content piracy costs over $500 million annually due to illegal redistribution of exclusive content, affecting major streaming platforms such as BeIN, Shahid, and OSN+.
- Pirates are increasingly attacking streaming platforms to steal content from live channels, building business models using that content and becoming illegal "super-aggregators".

> At the end of 2024, Italian authorities shut down a €3bn-a-year streaming piracy ring, which had more than 22 million subscribers in Europe, redistributing live and on-demand content from DAZN, Netflix, Amazon Prime, Paramount and Disney+, and other streaming services. The total damage to various streaming services was estimated at €10bn by Italian authorities.

> In July 2025, five people were sentenced for up to 7 years in prison for operating one of the largest illegal subscription-based streaming services in the US – Jetflicks – based in Las Vegas. The service allows tens of thousands of paid subscribers to stream and download TV content without permission from copyright holders. The value of the copyright infringement was estimated at 37.5 million USD.

### Waka TV Case

A recent case of combating piracy was a successful operation of MultiChoice and its subsidiary Irdeto against Waka TV – an illegal subscription-based IPTV service, which is mimicking a legitimate service while offering unauthorised access to both live and on-demand premium content.

The major South African Pay-TV operator, in collaboration with South African law enforcement, has conducted multiple raids, resulting in the arrest of thousands of individuals connected to the pirate network. MultiChoice continues to pursue both resellers and customers of Waka TV.

Sources: IABM, EY India, IAMAI, ASBU Quarterly Magazine, Financial Times, The Business and Financial Times, MultiChoice, US Department of Justice

# Content Protection

## Sports piracy is leading to revenue loss

- Sky and DAZN are among the most affected sports broadcasters, which is undermining their ability to acquire sports rights.
    - In May 2025, DAZN terminated its 5-year contract with Ligue 1 – Europe's fifth-biggest league in terms of club revenue – during the first year due to revenue losses and subscriber acquisition challenges. The broadcaster cited failure to combat piracy as a key reason for lost revenue. DAZN agreed to pay a €100m breakage fee.
- Pirated streams are being redistributed via various social networks, multiplying the damage to broadcasters' and rights holders' revenues.
- Another threat that contributes to the growing sports piracy concerns is the use of illicit streaming devices, such as Amazon Fire TV Sticks. Sky revealed that 59% of people in the UK who said they had used pirated feeds in the last year using a physical device said they used an Amazon Fire TV Stick.
- Content owners and rights holders are concerned about the vulnerability of older devices, which are lagging behind the rapid digital transformation in terms of security.

End-User at The Financial Times' Business of Football Summit

*Media-rights deals have been done on the basis of exclusivity, but I think there's almost an argument to say you can't get exclusive rights anymore because piracy is so bad.*

Tom Burrows
Global Head of Rights
DAZN Group
(February 2025)

Sources: IABM, Financial Times

# Content Protection

## Strategies to address piracy

### Using multi-DRM solutions

Multi-DRM solutions are the primary strategy to address piracy in today's fragmented digital landscape. While traditional broadcasters have a custom workflow for content distribution, often tied to a single vendor, there is a growing demand from OTT players for multi-DRM solutions in combating piracy: "*The first business is definitely the multi-DRM. The volumes are bigger and bigger. All the customers we're talking [to] – it's a billion of licenses per year.*" – *Pierre-Alexandre Bidard, Viaccess-Orca.*

### Analysing data to detect piracy

Artificial intelligence (AI) is increasingly used for search and classification to automate illegal content detection by gathering and analyzing metadata from back-end components integrated into a video platform. MediaTech suppliers employ AI for behavioral analytics to identify unusual requests, which leads to cease-and-desist orders being issued to illicit streamers and the shutdown of illegal streams.

### Collaborating with CDNs

Broadcast and media companies are increasingly collaborating with CDNs to combat piracy by integrating anti-piracy solutions directly into the content delivery infrastructure and adopting standards to manage multi-CDN content delivery. Collaboration and open standards are accelerating technology adoption and reducing fragmentation in streaming workflows.

**Content steering standards**
DASH-IF Content Steering standard (ETSI TS 103 998) provides a standardized, interoperable way for streaming providers to dynamically manage content delivery across multiple CDNs.

**Minimally intrusive access management systems** are increasingly used by CDNs to detect and block abnormal access patterns, degrading the quality of service for suspected pirate users without affecting legitimate viewers.

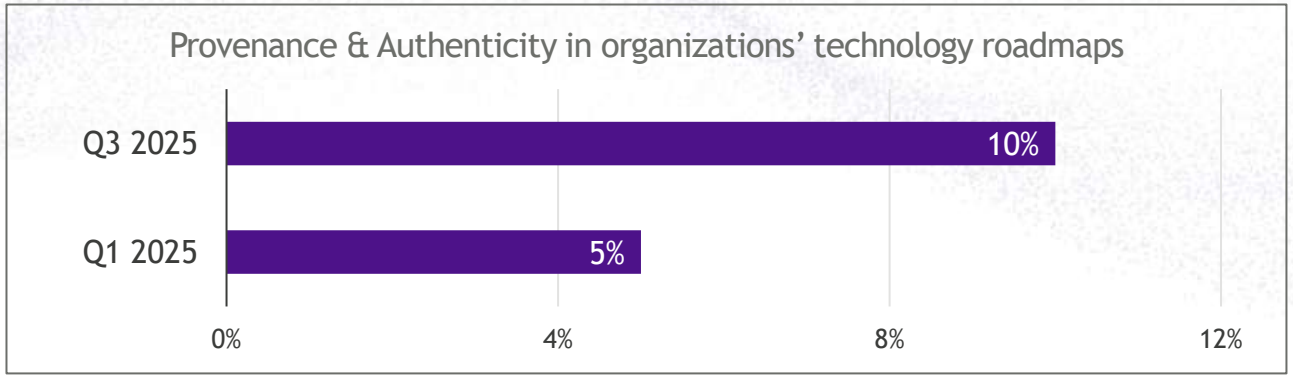
Source: IABM

# Content Protection

## Provenance and authenticity

- The rapid proliferation of generative AI tools has resulted in a surge of synthetic media, including deepfakes and tampered content, posing a significant threat to audience trust. This trend is driving investment in content provenance and authentication technology, which evolved from watermarking and fingerprinting. Provenance and authenticity is being used to identify content origin (camera, software, AI model), verify content authenticity and integrity, and trace content distribution.
- In response to this trend, IABM has introduced "provenance & authenticity" as an area of investment for technology roadmaps in the 2025 editions of the MediaTech Industry Tracker. Our data shows that the importance of provenance & authenticity in technology roadmaps increased from 5% at the beginning of the year to 10% in Q3 2025.




Source: IABM

MediaTech Supplier in an IABM interview

*There are a lot of companies in the industry that are looking at how to use technology to prevent that kind of disinformation [deepfakes, synthetic media] and **tracking content provenance from glass to glass**, from the moment it is recorded by a video camera up to the distribution to make sure that you can **trace the origins of that content throughout the entire process**, so capturing, possibly editing, encoding, transcoding, packaging of both live and VOD content **so that the client can verify** that the content comes from a **reputable source** and has not been modified throughout or has not been generated by an AI engine, video engine.*

Rodrigo Fernandes
Product Director Content Security
Irdeto
(June 2025)

# Content Protection

## Provenance and authenticity - open standards

The Coalition for Content Provenance and Authenticity (C2PA) is the first open technical standard for digital content provenance and authenticity, formed through an alliance between Adobe, Arm, Intel, Microsoft and Truepic. The standard is gaining traction due to the collaborative nature of the initiative. Project Origin's developments for news and Adobe's Content Authenticity Initiative (CAI) for creative community were combined at an early stage of development to work collaboratively rather than compete and ensured compatibility with a newer standard, JPEG Trust. Government endorsement would further accelerate C2PA adoption.

**Coalition for Content Provenance and Authenticity (C2PA)**

**Content Authenticity Initiative (CAI)**

Focuses on systems to provide context and history for digital media

Adobe

C2PA

**Project Origin**

Tackles disinformation in the digital news ecosystem

Microsoft BBC

While the first C2PA roll outs are focusing on detecting altered and synthetic content, the rapid proliferation of generative AI is likely to increase the need for standard traceability of content origin – from technical provenance to editorial provenance.

Source: IAMT, Coalition for Content Provenance and Authenticity

# Content Protection

## Provenance and authenticity

Currently, C2PA effectively addresses the issue of synthetic media proliferation but has limitations in tracing originator identity.

**Lack of editorial provenance** → **Lack of government endorsement**

### Technical provenance

**Required part of the C2PA protocol**

- Technical provenance enables verification of content origin, whether it was created with a camera or generated by AI. Technical metadata is all signed with a complete certificate chain.
- Technical provenance does not verify identity of content creation and whether the camera belongs to a legitimate source, such as an accredited news organization.

### Editorial provenance

**Optional part of the C2PA protocol**

- Editorial provenance is handled separately from technical provenance. Manufacturers of players are not obliged to validate the legitimacy of editorial content in order to claim C2PA compliance and are reluctant to implement optional parts of protocols.
- The lack of editorial provenance is seen by news organizations as a major threat to audience trust and a big challenge for the upcoming years.

Government endorsement is seen by news organizations as a necessary step in accelerating of adoption and implementation of C2PA. However, this endorsement is seen as beneficial when editorial provenance is at the same level as technical provenance, when not only technical metadata is verified but also identity of content originator.

Source: IABM

# Content Protection

## Provenance and authenticity – blockchain initiatives

Blockchain is becoming a part of the provenance and authenticity ecosystem, as some open-source initiatives and start-ups are developing blockchain-based solutions for digital asset provenance and authenticity.

| | Company Overview | Media Companies | Streaming Platforms | Production Companies |
|---|---|---|---|---|
| **Numbers Protocol** | A proprietary blockchain-based platform that registers digital assets on a decentralized ledger, creating an immutable, cryptographically signed record of content origin, edits, and distribution, enabling content traceability and verification. This technology serves as an alternative to C2PA but can potentially be integrated to or mapped with C2PA content credentials. | Can be used by media companies, and particularly news organizations, to register, track and verify content authenticity, addressing misinformation and copyright infringement. | Can support transparent licensing and rights management by enriching digital content with verifiable provenance. | • Registering and timestamping original content at the point of creation and provide verifiable proof of ownership<br>• Tracking content usage, licensing, and distribution across platforms<br>• Integrating with DRM and monetization systems |
| **Starling Framework** | An open-source blockchain-based system developed by the USC Shoah Foundation and Stanford University, which uses cryptographic hashes and blockchain for digital media authentication. | Media companies can use this system to document the origin and trace editing and distribution of news footage and user generated content (UGC) to ensure authenticity of digital content. | Can be used by streaming services to ensure that distributed content is authentic and unaltered. | • Authenticating and preserving content from creation to archiving<br>• Provide verifiable evidence of content authenticity<br>• Enabling content provenance |

Sources: IABM, Numbers Protocol, Starling Lab

# Talent

## Talent shortage in securing MediaTech ecosystem

The talent pool in the broadcast and media industry is very limited as the industry transitions to IP-based workflows and cloud environments, resulting in the convergence of broadcast and general IT workflows.

Main challenges:

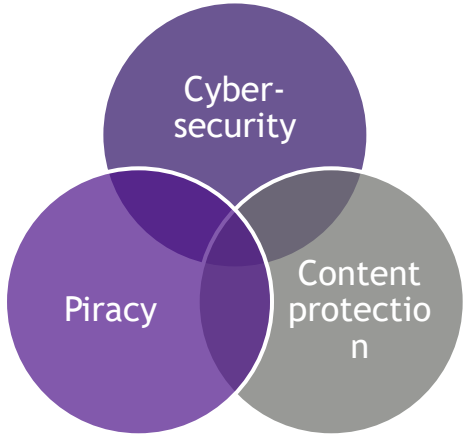
- Managing and troubleshooting IT infrastructures within broadcast environments, particularly in live production.
- A shortage of talent with network-specific knowledge for content security.

**Broadcast & Media Talent Pool**

The industry faces a shortage of broadcast engineers with expertise in cloud security, vulnerabilities of IP-based workflows, and AI threat mitigation. There is also a lack of solution architects and product managers with security knowledge.

**Cybersecurity Talent Pool**

IT engineers typically struggle to respond to incidents in real-time within live environments, particularly during major sporting events production.




The boundaries between content protection, anti-piracy and cyber-security are increasingly blurring, challenging media technology vendors to balance insourcing and outsourcing security talent. IABM's research shows that both vendors and end-users primarily insource their security expertise while outsourcing specific functions. Core security operations – such as R&D, content file uploading, CDN management, and enterprise cybersecurity – typically remain in-house. Meanwhile, specialized services like emergency cybersecurity resources can be outsourced.

Source: IABM

# Talent

## Strategies to address talent shortage

### Insourcing strategies

- Continuous training and upskilling of internal staff, including functions such as solution architecture and pre-sales.
- Recruiting and training talent from the industry that have either security or domain expertise, including talent with traditional broadcast expertise transitioning to OTT and streaming.

### Outsourcing strategies

- Relying on security consulting from companies that have expertise, using them as contractors.

MediaTech Supplier in an IABM interview

*Many broadcast engineers find IT challenging, but now they need to excel at it. We've got a lot of IT technology in the production facility and that's only going to accelerate with the move to software-defined production and – as outlined underneath the Dynamic Media Facility work of the EBU – is the future, and it's going to require a completely different set of skills.*

John Naylor
VP Product Security and Ross Research Labs
Ross Video
(July 2025)

Source: IABM

# Future Outlook

**Connect. Support. Inform.**
theiabm.org

# Future Outlook

## Content Provenance and Authenticity

- Deepfakes and tampered content represent a new kind of threat in the industry. While AI offers powerful capabilities to enhance content protection and infrastructure security, such as automated threat detection, anomaly identification, and real-time incident response, it is increasingly being used to alter content with malicious outcomes, and cyber attacks of this nature may remain unnoticed.
- Content authenticity is crucial for retaining viewership, particularly in live news and sports – including betting, which is becoming part of the live sports sector. In the next few years, media companies are likely to invest in internal security systems that would validate signatures on content. All the ingested content is expected to have signed provenance, such as C2PA signatures or potentially crypto chains. The focus seems poised to shift from device to identity verification to ensure that content comes from trusted partners.
- Currently, streaming and social media are the most affected, but there is a growing concern that altered content may become a significant threat for DVB, cable TV, and ATSC in a few years.
- Development of provenance tools requires a holistic approach and collaboration between CDN companies, security organizations, cloud service providers and industry bodies.

*Pirates are now using extremely powerful tools.* ***The big thing is deepfakes.*** *They can hack the content.*

*You can now take legal content and change it.* ***And this is the biggest fear that we receive.***

*AI can be used as a tool, but, unfortunately, right now it's more used to trying to create content that that has been altered […]* ***Within a few years, that's going to be a major topic.***

***The biggest challenge is going to be fighting AI, fighting fakes,*** *telling apart generated videos from real ones.*

Source: IABM

# Future Outlook

## Migration toward Dynamic Media Facility

The migration toward EBU's Dynamic Media Facility (DMF) offers the MediaTech ecosystem both transformative opportunities but also escalates critical security challenges over the next two to three years. Key drivers of DMF adoption include:

| | |
|---|---|
| **Agility and Resilience** | DMF’s software-driven design allows media organizations to establish backup systems and quickly shift production between facilities during failures – a critical capability for live production environments. |
| **Open-Source Ecosystem** | The transition from proprietary Dynamic Media Facility frameworks to open-source solutions, particularly with the Linux Foundation's Media eXchange Layer (MXL), is accelerating DMF adoption potential throughout the broadcast and media industry. |
| **Multi-Tenancy Isolation** | DMF enables secure collaboration, so that different teams can operate within the same infrastructure without compromising each other’s content or production workflows. |
| **Zero Trust Architecture** | As cyber threats multiply due to expanded IP and cloud environments, Zero Trust adoption has evolved from a best practice to an operational necessity for major organizations. Zero Trust principles are integral to securing DMF architecture across all its architectural layers. New regulatory and compliance requirements further drive Zero Trust architecture adoption across the industry. |

Source: IABM

# Future Outlook

## Long-term prospects – quantum computing in securing broadcasting workflows

While quantum computing remains in its early developmental stages, several initiatives of quantum technologies are underway across Europe. Regulatory support plays a crucial role in developing these quantum infrastructures. Recent advances in quantum technologies promise significant benefits for ultra-secure communications, which could impact broadcasting in the long term.

### Quantum Europe Strategy

- On July 2, 2025, the European Commission released a document outlining its strategy to position Europe as a leader in quantum technologies through coordinated research, innovation, infrastructure and skills development.
- The European quantum strategy outlines the **European Quantum Communication Infrastructure (EuroQCI)** initiative, which offers ultra-secure data transmission, protects critical infrastructures, and safeguards sensitive information against future quantum-enabled cyber threats. It is actively deploying cross-border terrestrial quantum links and establishing ground stations for space-based Quantum Key Distribution (QKD), which will result in a fully interconnected secure experimental network combining terrestrial and satellite segments by 2030.
- Quantum communication enables the establishment of quantum communication networks necessary for interconnecting quantum devices such as sensors and computers, into a so-called “Quantum Internet”. The **Quantum Internet initiative** in Europe has demonstrated quantum networking at the metropolitan scale and will launch a pilot facility in 2026 to test quantum-safe components and early use cases, including secure quantum-cloud services and distributed computing. This establishes the foundation for a federated quantum Internet by 2030.

### BRIDGE Quantum Call 2025

Switzerland has recently launched the BRIDGE Quantum Call 2025 – a funding initiative which aims to advance applied research with partners targeting practical quantum communication applications. Specific planned pilot programs will arise from projects funded through this call starting in late 2025 and beyond. This initiative demonstrates ongoing efforts to move toward practical quantum deployments in communications, including broadcast ecosystems.

Source: IABM, European Commission, Swiss National Science Foundation

# Powerful business intelligence

**Play it smart. Get ahead.**

insight@theiabm.org