Publication date:
Jan 2025

Authors:
Fernando Montenegro
Thomas Thomson
Rik Turner

API Security Is Now Key to Securing M&E Workflows

Commissioned by:

Contents

Summary

The security landscape for media and entertainment (M&E) organizations is evolving quickly, and the attack surface is increasing as the video pipeline moves to software and cloud native deployments. This means a careful assessment of how the ballooning number of APIs that support software applications can be managed is needed, because it is vital to protect critical business systems and to secure the valuable IP of media organizations.

Even though the number of APIs, both internal and third party, runs well into the thousands for many organizations, responsibility for API security is spread across teams. This has caused uncertainty over the visibility that organizations have over APIs and how to protect media workflows. API security deployments are piecemeal, and some organizations see themselves as falling behind on what they believe to be a critical gap in their architectures.

In a recent survey of 160 M&E organizations comprising broadcasters, pay TV operators, over-the-top (OTT) service providers, and social media platforms conducted by Omdia, more than half of respondents reported significant difficulties in implementing API security within their operations. Protecting media workflows was their top priority, but finding the right solution has been challenging: study participants either reported that solutions are expensive or indicated their organizations have a low conceptual awareness of API security.

It is of paramount importance that video service providers (VSPs) address the gap between their increasing API usage and the implementation of proper security measures. This gap is brought into sharp focus as the overwhelming majority of respondents reported not having visibility into two-fifths of their internal API use. This creates significant vulnerabilities. To address this, VSPs should prioritize solutions that support easy implementation and offer a broader feature set beyond mere visibility, such as risk and compliance auditing and API testing.

M&E buyers must therefore concentrate their efforts on integrating API security into workflow areas where adoption is likely to generate the most fruitful return on investment. They should coordinate security across API and cybersecurity in addition to content security. Security solutions that both secure the enterprise and protect revenue will provide a meaningful ROI. For this reason, security solutions are not a cost sink but a strategic necessity worthy of prolonged investment.

Introduction

M&E companies have understood the growing need for content security. It plays a vital role in monetizing video content by preventing unauthorized viewing, tampering, and redistribution. Content security has become more complicated and crucial to ensure returns on the substantial investment made in content production and acquisition as the broadcast and pay TV industry has shifted toward direct-to-consumer streaming. The demand for end-to-end solutions that protect evolving streaming infrastructure presents a challenge to VSPs looking to migrate away from componentized security solutions (which focus on discrete elements of the video workflow) to a more holistic approach that offers much more full-service visibility across an increasingly fragmented landscape, particularly with respect to devices and distribution infrastructure.

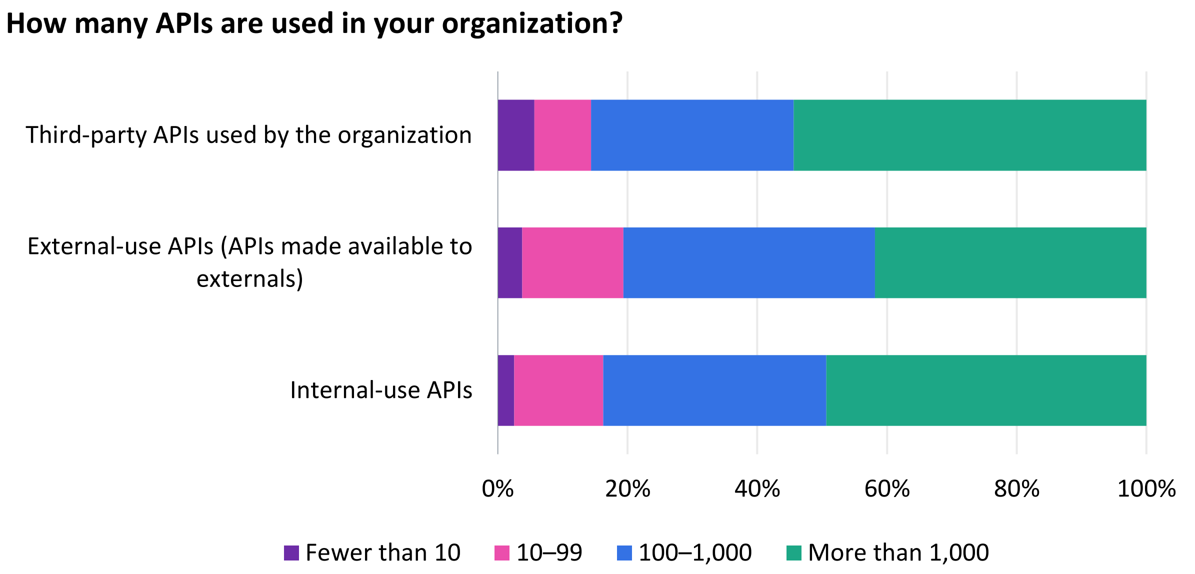
There is a much broader attack surface now. In the siloed world of linear broadcast infrastructure, content providers had relative peace of mind about tampering, hacks, and data breaches. An operator and associated security vendor managed the encryption at the set-top box (STB) level, and anti-piracy had a much stronger preventive component. In streaming native workflows, piracy is one of many other kinds of security problems that a media organization must contend with, and the onus is now on the provider itself to protect, for example, its content delivery network infrastructure, production and postproduction workflows, and the video-processing stack; to prevent distributed denial-of-service (DDoS) attacks; and to manage other security needs. Media organizations require the right tools to adapt to the increasing sophistication of threat actors and need to develop strong solutions to defend against an expanding range of attacks.

This widening attack surface has been enabled by increasing deployments of software-based video components away from dedicated on-premises infrastructure. The value of these newer deployments is well understood in technology markets, and M&E is no different. It offers flexibility, a reduction in the total cost of ownership, and ease of operations. The proliferation of software-based services was at least in part made possible by APIs, because they simplify the integration of different services. The number of APIs in use has thus mushroomed as the popularity of software-based services has soared.

APIs allow developers to easily code modular applications into the streaming stack, and leaning into a more developer-centric approach has been a crucial catalyst in streamlining video workflow integration, allowing media organizations to evolve away from black box, broadcast-exclusive tech silos. However, introducing these APIs to connect video workflow elements invites new security challenges such as exposure to vulnerabilities that emanate from insecure APIs. These challenges include authentication and authorization issues, business logic flaws, and data exfiltration.

In the last few years, we have seen a massive expansion in the entire digital value chain with the rise of software as a service (SaaS) vendors supporting M&E workflows. The trend is for all these participants in the value chain to use APIs to streamline workflow integration.

Figure 1: Number of APIs in use



Note: n=160

© 2025 Omdia

Source: Omdia

Use of APIs is rising. At the same time, many of our respondents reported API security incidents with specific issues such as the exfiltration of internal records and large-scale data scraping.

This scenario means companies should improve their API security efforts now, because the increase in APIs will only continue, thereby compounding the security problems unless such steps are taken. As the number of APIs increases, the attack surface will continue to expand, resulting in even more potential attacks.

A quick primer on API security

The common flow for API security is centered around four main use cases that operate in an infinite loop, not unlike the build-ship-run-monitor cycle used in DevOps:

- **Discovery of APIs being used across environments:** This can be done in many different ways, including ingestion of OpenAPI (Swagger) definitions, scanning code repositories, and active scanning of environments. Most APIs are discovered by analyzing traffic. Uploading API spec files is a less-used tactic and is only possible when the organization already knows what APIs it has. Additionally, no one approach is sufficient: The combination of continuous traffic and repository scanning is likely to yield a comprehensive view of API usage within organizations.

  Organizations need to account for API security considerations across their entire technology estate, not just specific API-friendly environments. In many cases, handling legacy API usage requires a different approach.

- **Analysis of API security issues, making a distinction between API security posture issues (misconfigurations and vulnerabilities) and API runtime issues (actual attacks against the environment):** This involves mapping issues to standards or common lists such as the OWASP API Security Top 10. In many cases, it is not sufficient to just identify the issue—it also helps to contextualize it and prioritize accordingly. This prioritization is critical for both proactive (posture) and reactive (runtime) security.

- **Monitoring API security with detection and response:** Because APIs are deployed in production and used by both regular users and potential attackers, it is important to monitor API usage for signs of attacks. This is a complex stage that often involves integrating API security into both modern and legacy technology, ranging across packet captures and traffic mirroring, API gateway insertions, source code libraries, and more. As API usage telemetry is collected, it is analyzed and prioritized. Response actions include sophisticated orchestration across multiple technology elements.

- **API compliance and reporting:** Here, the objective is to efficiently and accurately report on the state of API security, both for internal operational purposes and to support external compliance mandates.

These use cases require not only technology components that can implement API security functionality, but also collaboration between teams, and specialized domain knowledge about secure design and development of APIs.

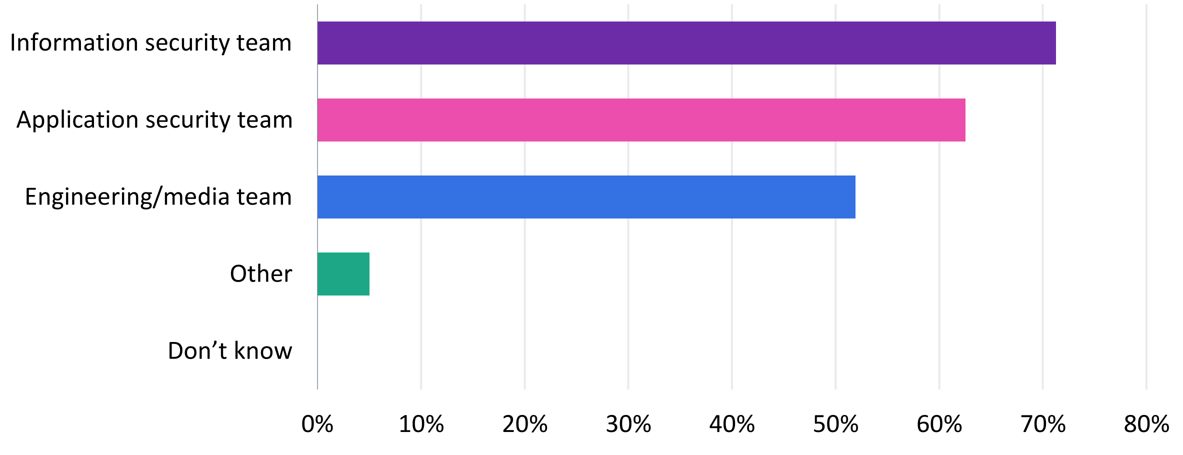
Adoption and perception of API security within organizations

Responsibility across teams

Like other areas of cybersecurity, API security occupies a middle ground within organizations. According to our research results, the three main teams involved in API security technology selection and ongoing management are information security, application security, and engineering/media.

Figure 2: API security internal domain ownership is spread across teams

Which teams are primarily responsible for technology selection and ongoing management for API security in your organization?



Note: n=160

© 2025 Omdia

Source: Omdia

The distribution in **Figure 2** is for the entire population of respondents. There were, however, differences by geography and industry:

- Respondents based in Asia and Oceania had application security teams at 83%.

- Respondents from OTT content delivery companies had engineering teams higher, at 71%. Those in social media, however, had application security teams at 82%.

These results have both positive and negative implications. On the positive side, the responsibility for API security being distributed across an organization's various teams means API security may receive broad organizational support. On the negative side, this distribution of responsibility may cause organizational confusion, overhead, and a lack of definitive accountability and progress.

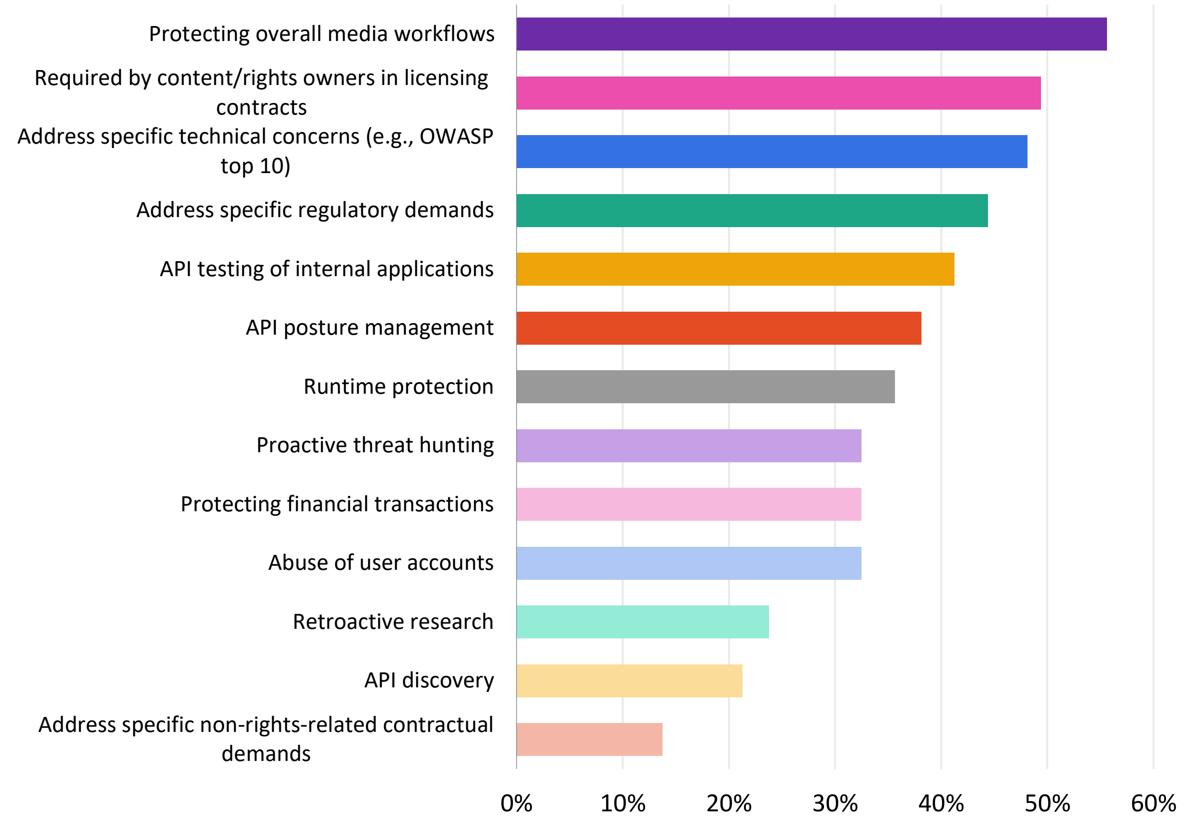
As organizations consider API security, it is important for them to clearly define roles and responsibilities. The following steps may facilitate this process:

- Assigning a dedicated API security team and fostering collaboration
- Establishing clear roles and responsibilities
- Implementing a centralized API security strategy

When usage is being considered, protecting media workflows is a key priority

When asked about their main priorities for API security, organizations responded with a mixture of business and technology drivers. The most common priority was protecting overall media workflows, reflecting an understanding of the importance of API security in the media creation and delivery value chain. In addition, the respondents noted external pressure from counterparties and regulatory agents as key motivators for strengthening API security.

Figure 3: Broad understanding of the value of API security in the media supply chain



Which are your top priorities for driving API security at your organization?

Note: n=160

© 2025 Omdia

Source: Omdia

The motivators for strengthening API security differed substantially based on subsection:

- Respondents in both Asia and Europe rated regulatory concerns as a higher priority, at 56% and 52%, respectively. Latin American respondents rated runtime protection more highly, at 50%.
- For OTT service respondents, regulatory concerns were highly ranked at 62%, and respondents in broadcasting and social media ranked addressing specific technical concerns highly, at 60% and 58%, respectively.
- Respondents with more experience in API security ranked abuse of user accounts higher (39%) than did the respondents overall (33%).

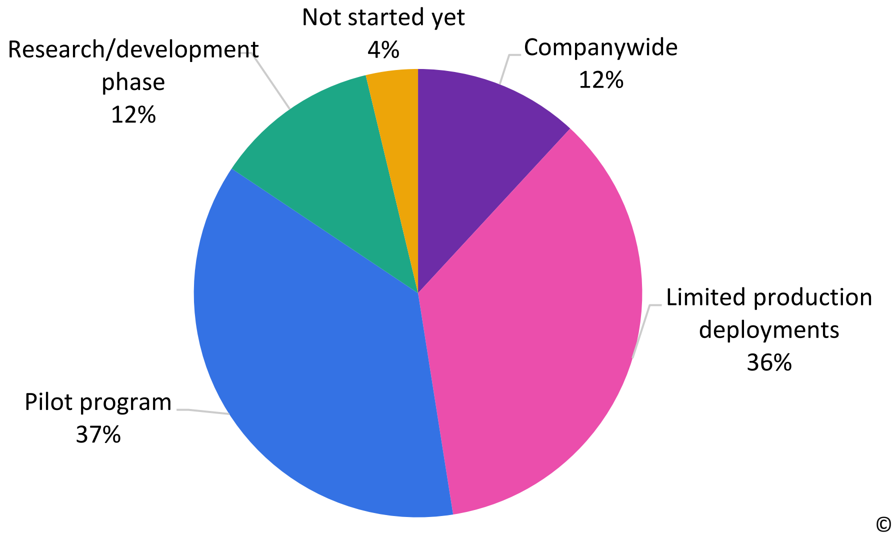
These results indicate that while there is a broad consensus around the importance of protecting workflows, organizations looking to implement API security initiatives will likely need a more customized approach to aligning their efforts with their business needs.

Most organizations have adopted or are working on adoption

When asked about the progress of their API security implementation, most organizations reported that they were in either the pilot project stage or some level of production implementation.

Figure 4: Mixed levels of API security implementation

Which best describes the scope of API security adoption in your organization?



Note: n=160

© 2025 Omdia

Source: Omdia

Notable segment differences include the following:

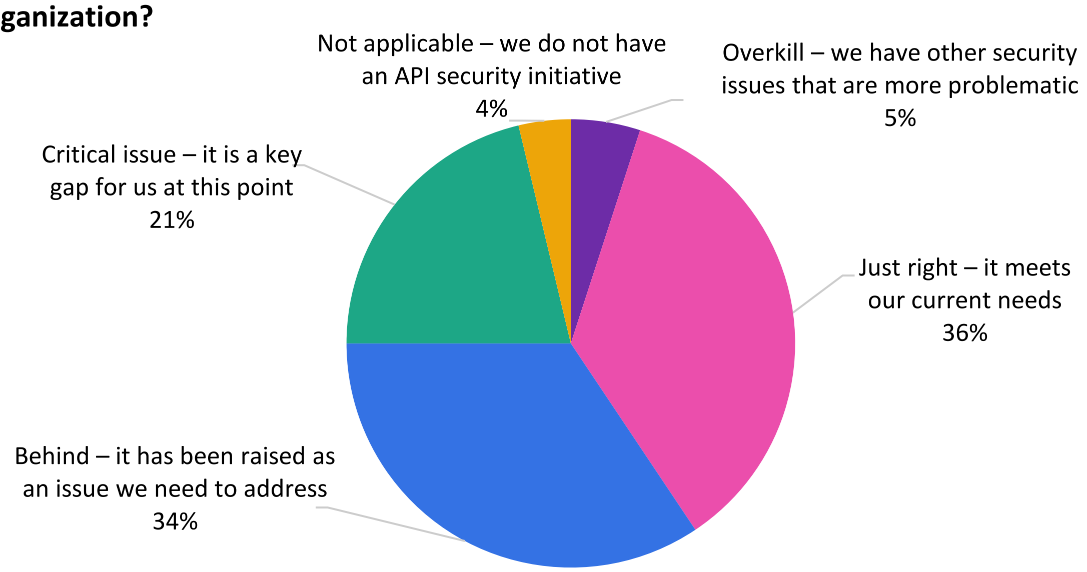
- North American respondents reported much higher levels of production deployment, at 65%, compared with 48% worldwide.
- Latin American respondents reported a paltry 13% in production. As with most enterprise technologies, in cyber and beyond, North America is usually the lead adopter, and in the case of cyber in particular, it reflects that region’s heightened awareness of security issues as a result.
- Respondents in the $500 million and lower range reported production levels of only 29%, whereas larger respondents appeared further ahead, with 83% indicating some level of production deployment. This result is expected given that larger organizations tend to have more exposure to cyber risks and larger security teams and budgets.

Most companies are behind on implementation of API security

Though many respondents indicated some level of progress toward API security implementation (**Figure 4**), a significant portion of the respondents indicated that progress was less than desired; 51% said they were either behind or saw it as a critical issue (**Figure 5**).

Figure 5: How organizations view their API security implementation

How does your API security deployment compares with other security initiatives in your organization?



Note: n=160

© 2025 Omdia

Source: Omdia

Notable segment differences include the following:

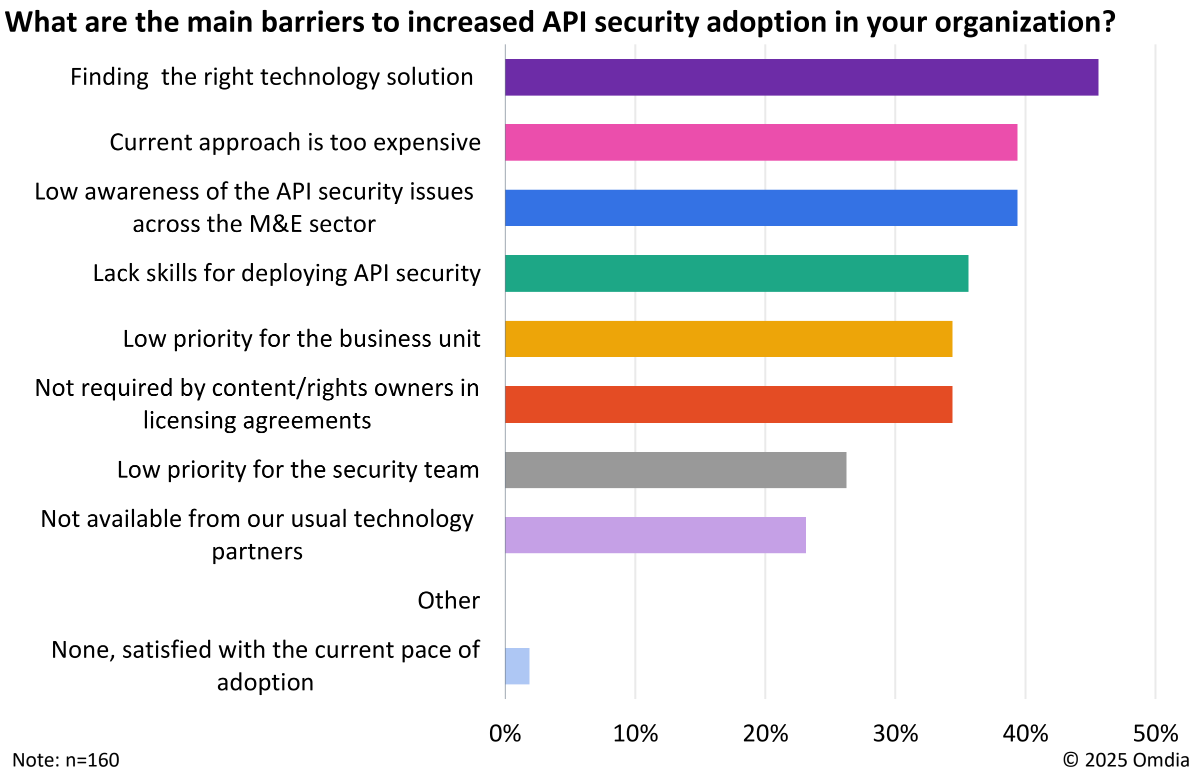
- Latin American respondents were aware of their slower implementation progress; 75% acknowledged being behind.
- Those in pay TV also indicated being behind or a critical gap, at 72%.
- Respondents from larger organizations ($1 billion or more in revenue) appear more at ease with their pace of deployment: 63% indicate it is "just right."

Finding the right tech and rightsizing it are major barriers

The respondents identified the following factors as the top three obstacles to increased adoption:

- Finding the right solution is difficult.
- The current options are too expensive.
- Overall awareness of the importance of API security is low.

Figure 6: Perceived hurdles to API security adoption are widespread



Source: Omdia

Notable segment differences are as follows:

- Respondents in Asia identified solution costs as the most critical issue, at 51%. In North America, finding the right solution was the most critical issue, at 60%. In Latin America, Europe, the Middle East, and Africa, the main issue was lack of awareness.

- Among the larger respondents ($1 billion or more in revenue), 48% indicated that they did not see API security as a requirement in their licensing agreements.

Putting these answers together, the picture that emerges shows that there are several organizations with efforts underway with API security, but they are often hitting a combination of technology roadblocks such as finding the right solution or simply a perceived lack of urgency for the topic. Organizations should understand that the potential damage from a single API incident can be significant. This should factor into the ROI considerations for API security projects.

API security needs

API security starts with visibility

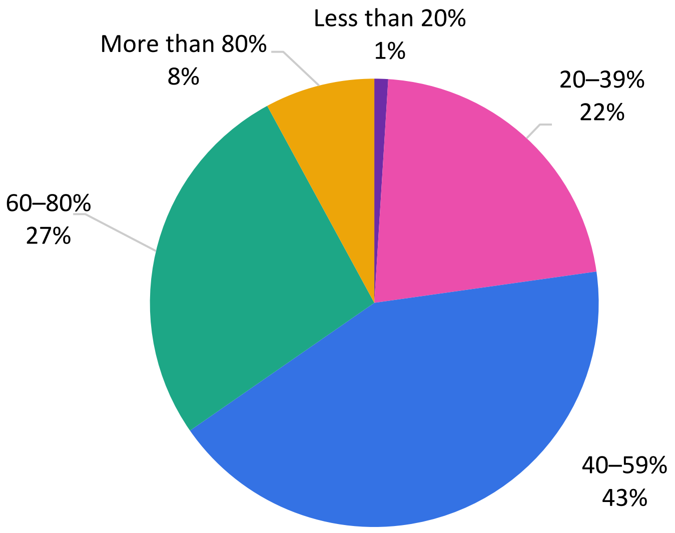
As with many security technologies, proper visibility is the first step. This is prudent; whether thinking about the popular proverb “look before you leap” or considering more structural methodologies such as OODA (observe, orient, decide, act) loops, it is important for organizations to consider current state for security implementations as they decide on next steps.

API security is no different. According to our research, visibility often emerges as a popular first step among respondents. However, the results also indicate API visibility.

Figure 7 depicts an estimation of the respondents’ visibility into their overall API usage. Only a small fraction (8%) of respondents indicated that they had visibility over more than 80% of their traffic, with a significant majority (70%) reporting visibility into 40% to 80% of their traffic.

Figure 7: Awareness of API usage

What percentage of your organization’s total API usage are you aware of?



Note: n=160

© 2025 Omdia

Source: Omdia

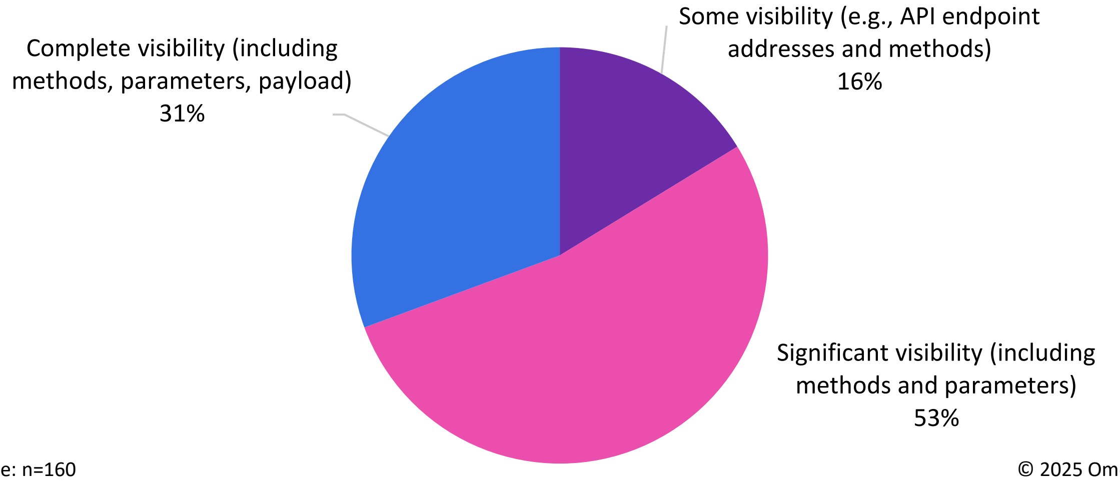
The results appear consistent across segments, with some minor variation:

- Only 3% of respondents in Latin America reported more than 80% visibility, with 81% reporting 40%–80% visibility.
- Broadcasting and social media respondents reported slightly higher visibility levels but not significantly so.

Another dimension to consider is how deep that visibility is. Here, the picture that emerges is slightly more positive: More than 31% of respondents said that they had complete visibility of their traffic.

Figure 8: Depth of visibility

Which best characterizes the visibility you have over the traffic shared between APIs at your organization?



Note: n=160

© 2025 Omdia

Source: Omdia

In terms of regional differences, Latin America lagged behind on the depth of their visibility, with only 19% of respondents reporting complete visibility.

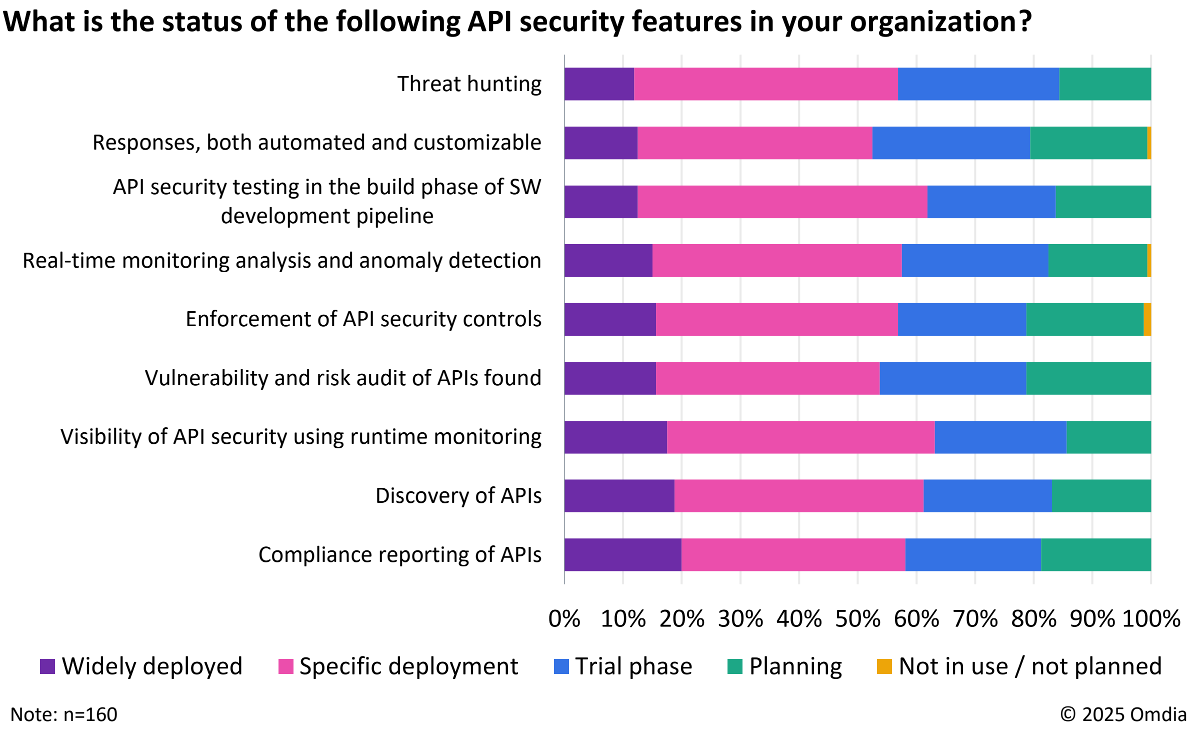
Highlighting an undercurrent of potential disconnection between senior managers in an organization and their teams, 41% of respondents that self-reported as VPs or above indicated that they had complete visibility.

Digging into details: A broad selection of needs

Though visibility is often the primary concern and a first step for many organizations when tackling API security, visibility alone is not enough. Once found, APIs must be assessed, secured, and monitored.

According to survey respondents, as can be seen in **Figure 9**, all of these areas have broadly the same level of progress for those that are deploying API security. Visibility-related features have slightly more developed implementation progress than others, but not by much.

Figure 9: Organizations’ deployment progress for each API security feature



Note: n=160

© 2025 Omdia

Source: Omdia

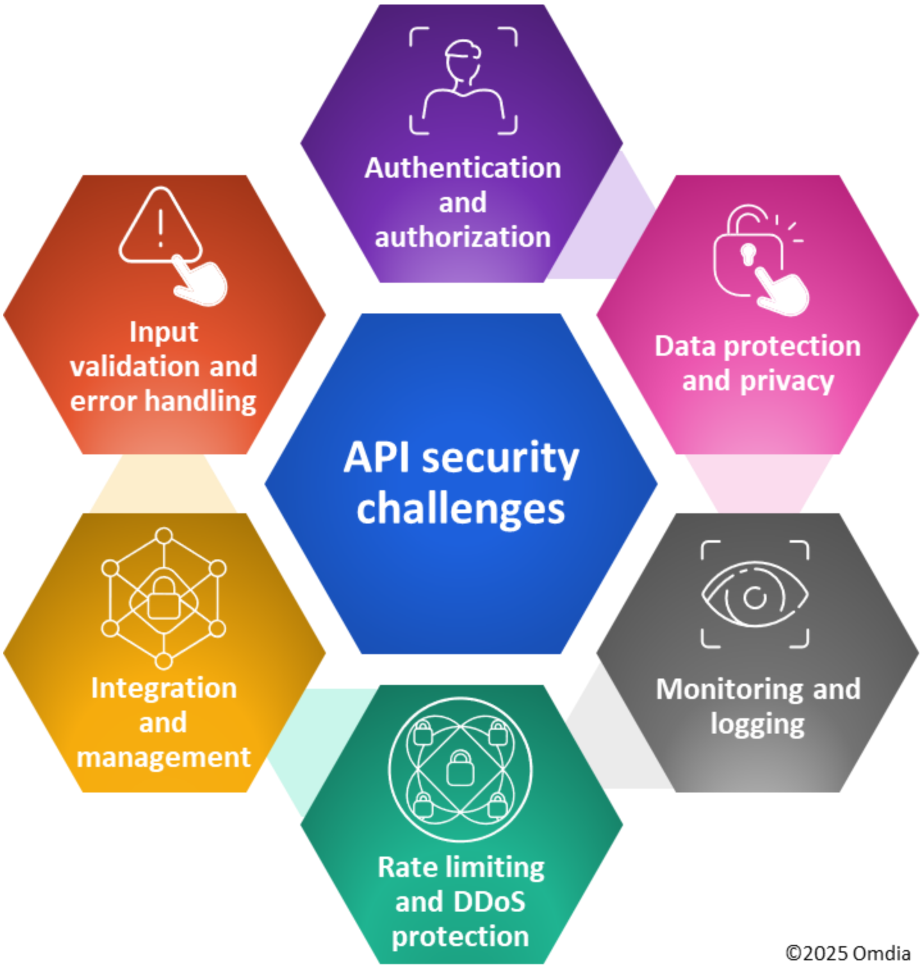
Reflecting a common theme throughout our research, North American respondents reported wider deployment of all features, and Latin American respondents reported less.

One area worth highlighting is the need for compliance. Regulatory demands are not often top of mind for organizations, but they should be. The Federal Communications Commission (FCC) is known to fine organizations for failure to protect customer information. In one recent case, a company was breached three times because APIs were insecure.

The protection of customer data (directly or indirectly) has to do with APIs that exchange this data. So even if regulations do not explicitly mention API security, a breach due to misconfigured APIs or lack of API protections can result in noncompliance with the data privacy regulations. More organizations need to be aware of this connection.

The survey also revealed several challenges that the respondents faced in implementing API security (**Figure 10**).

Figure 10: Additional API security challenges run the gamut across security topics


Authentication and authorization
Input validation and error handling
Data protection and privacy
API security challenges
Integration and management
Monitoring and logging
Rate limiting and DDoS protection
©2025 Omdia

Source: Omdia

The list of challenges in **Figure 10** reflects how deeply API security can affect media workflows:

- Authentication and authorization are the essential aspects that support different entities exchanging information along the value chain because they ensure the confidentiality of assets and information. Improper authentication and authorization are primary vectors for API attacks. Adversaries look for public-facing APIs that exchange sensitive data but lack proper authentication and authorization controls, allowing them to steal that data.

- Data protection and privacy are needed in the context of risk management (i.e., how to protect assets) but also in light of regulatory mandates, particularly when transacting in Europe or with individual consumers.

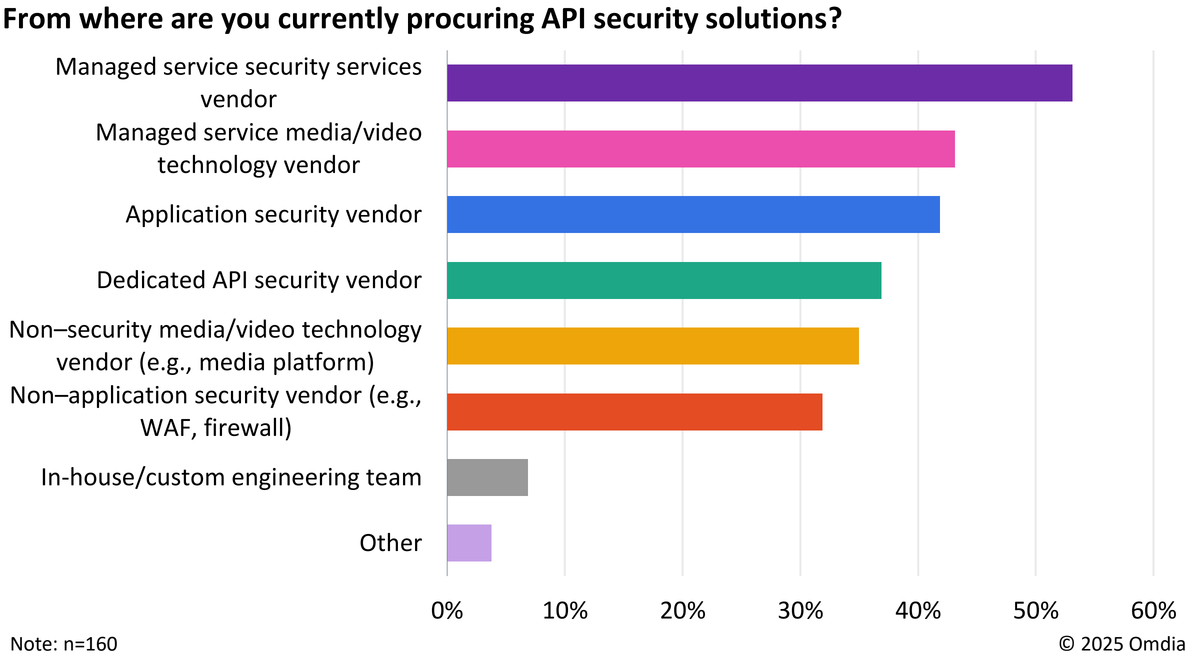
- Monitoring and logging are key to maintaining security and operational integrity once APIs are deployed.
- Rate limiting and DDoS protection are important to maintain operational integrity and availability. They are particularly important for APIs used in public settings, such as those supporting calls from mobile devices or applications.
- Integration and management ensure that API security efforts align within broader operational practices without adding undue burden.
- Input validation and error handling are critical functions that every API should implement, particularly to protect against malicious usage due to improper authentication and authorization protocols. In the realm of consumer access, for example, how well protected is an API against manipulation attacks from a user account that has been taken over by a malicious actor?

Tackling API and content security requirements

API and content security are not to be kept in organizational silos. Rather, they must be tackled together since they perform complementary roles as part of the wider enterprise security conversation.

When M&E organizations look at the procurement model for security services, they must assess their own ability to manage their critical content workflows in-house. Historically, developing these solutions is outside the core competencies of most VSPs, because it requires analyzing large amounts of user data and crafting actionable strategies to manage account sharing and device encryption. This means that buyers need partners to pivot their security solutions from being a cost to being revenue-generating technology.

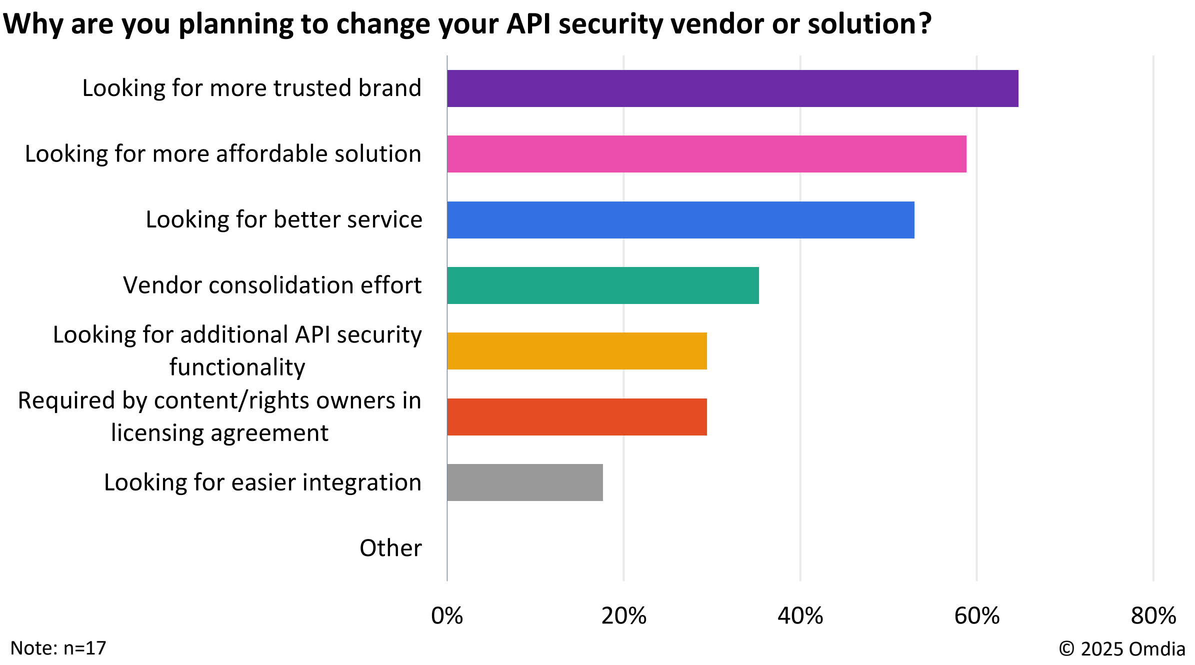
Figure 11: Organizations are looking at different types of API security solutions



Source: Omdia

Survey respondents indicated that they procured API security solutions from various sources. What stands out is the requirement to lean on partners in a very hands-on capacity, which was observed across the respondents. This is no surprise, given the clear incumbent preference for the managed service model, coming from either an enterprise security vendor or a media technology vendor with expertise in the security domain. In-house deployment was uncommon, reflecting the resourcing trade-offs that buyers see in building specialized security applications and teams internally.

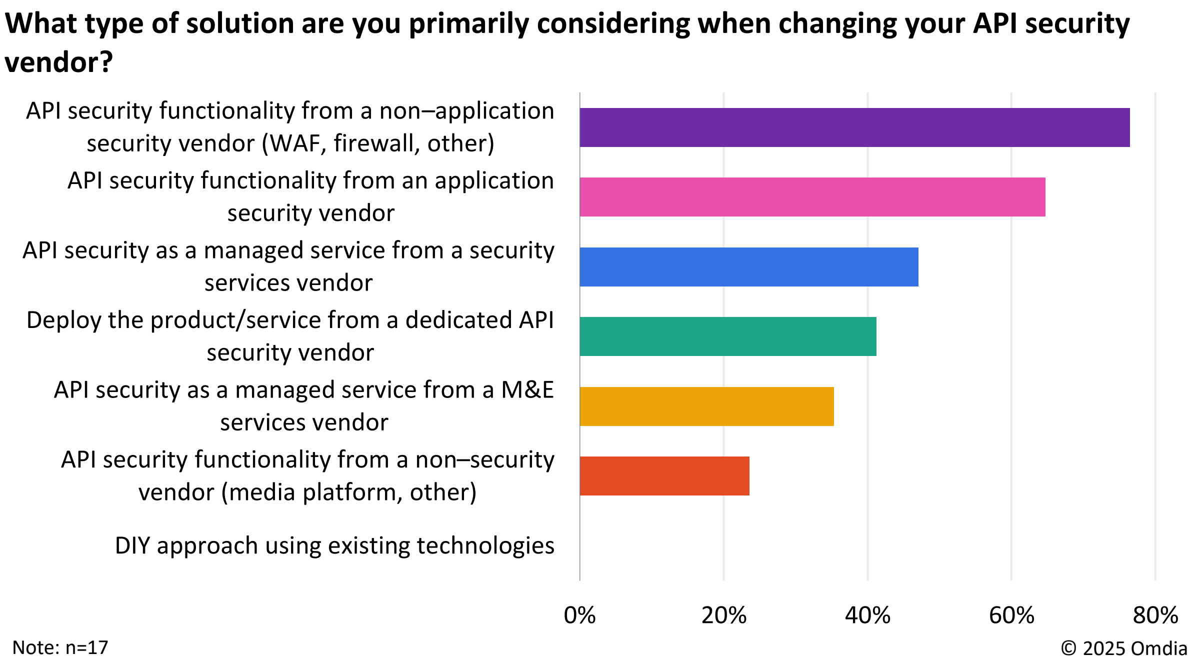
Figure 12: Reasons for changing API security solution vendor



Source: Omdia

Although affordability was a key concern, trust proved more important. In the realm of content security, buyer–vendor relations must be based on trust, given the fact that vendors will have access to and partial responsibility for critical systems and sensitive data. It is unsurprising, therefore, that buyers are seeking a trusted brand above all else.

Figure 13: Priorities in changing API security vendor

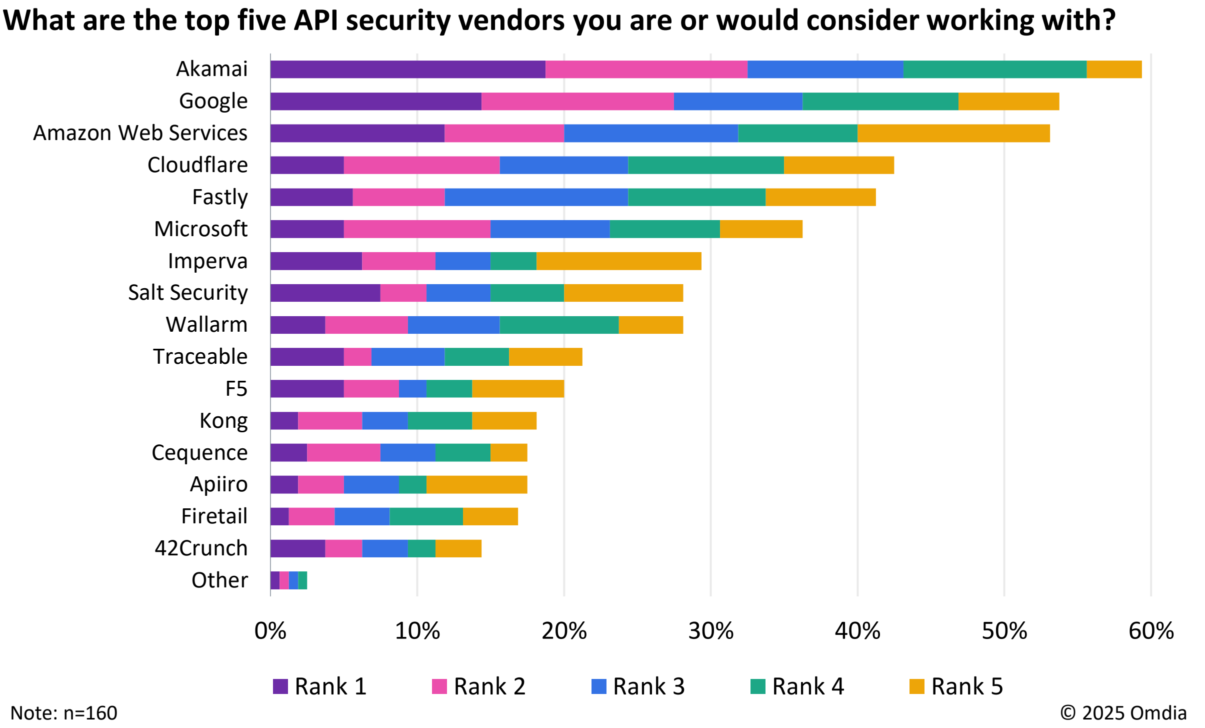


Source: Omdia

Looking ahead, buyers plan to prioritize ease of implementation with their next API security solution. This suggests that buyers are moving away from a managed service approach toward a much more modular one, buying specific API security functionality, either from a non–application security vendor (web application firewall [WAF], firewall, other) or from an application security vendor.

API security is often expected to be included in broader offerings and less so as part of a managed service. Vendors that can straddle both content security and cybersecurity are well positioned to benefit from this; most respondents indicated that they did not intend to procure API security solutions from specialized media technology vendors.

Figure 14: When vendors are being considered, the focus is on well-known platforms



Source: Omdia

The competitive landscape

Respondents cited a host of vendor options, some with a clearer background in cybersecurity and others with a history of providing adjacent services, such as content delivery or file and object storage.

Although enterprise cloud providers such as Google Cloud Platform (GCP) and Amazon Web Services (AWS) will be a key component of the API security landscape, vendors with strong experience and cachet in critical video transport tasks maintain a key advantage.

This explains the prominence of vendors such as Akamai (most notably) and Fastly in the results, both of which are highly experienced in serving media buyers across content delivery and security.

Where to start with API security

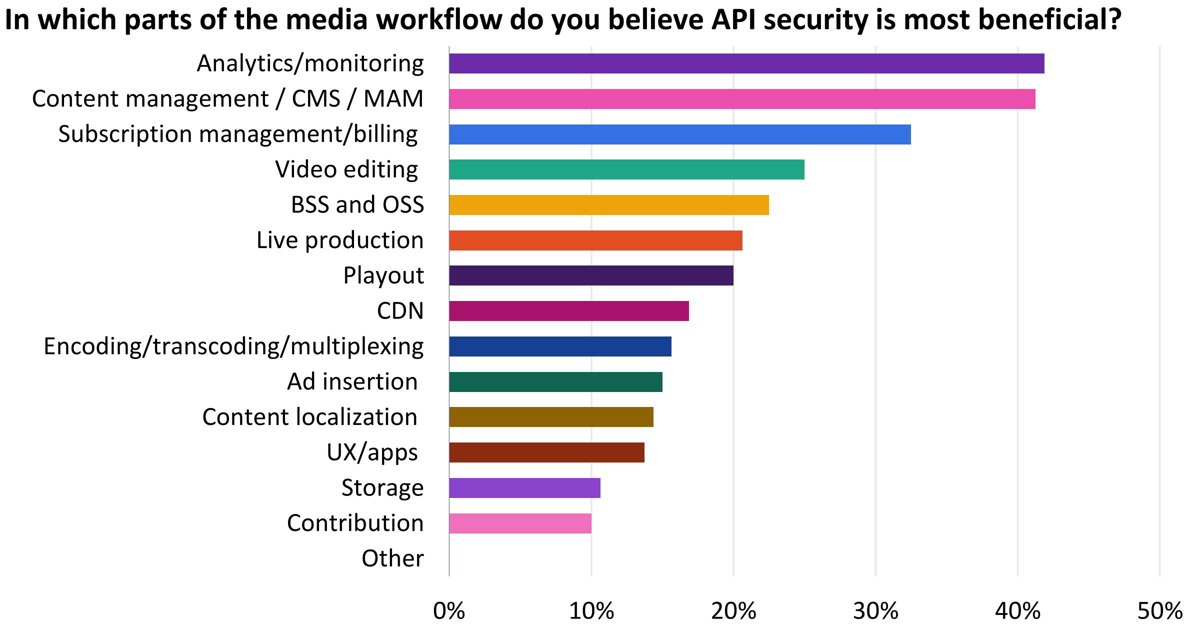
API security has numerous use cases in the media workflow, but the focus should be on the lowest-hanging fruit first.

API security should be integrated into workflow areas that have transitioned along with SaaS and cloud native deployments. By contrast, workflow areas with heavy on-premises components, such as contribution, may not benefit substantially from API security integration.

Analytics and monitoring present strong use cases for API security because these areas align most closely with the primary function of APIs: to stitch together workflow functions to improve orchestration of the broader platform.

Video editing is another key use case for API security. In a software native environment, threat actors can gain access to sensitive work-in-progress files if appropriate protections are not in place.

Figure 15: As API security is deployed, interest is on easy wins for M&E buyers



Note: n=160

© 2025 Omdia

Source: Omdia

North American respondents believed API security to benefit playout far more than did other respondents globally. This is because cloud playout is more prominent in North America and has supported the proliferation of free ad-supported streaming TV (FAST) channels; as a result, API usage is likely higher in that domain than in other markets.

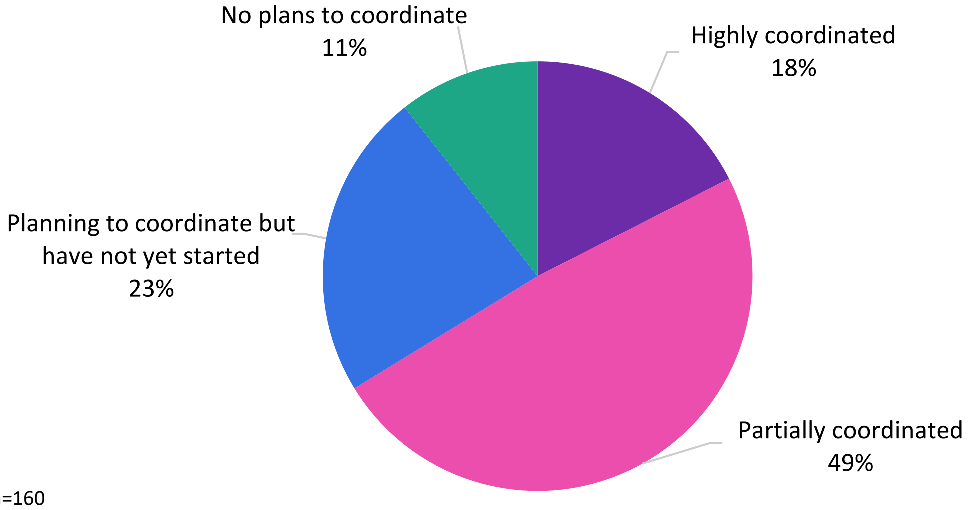
M&E buyers should focus on integrating API security into workflow areas that are likely to generate the most substantial ROI.

Content security is a parallel concern

Across all buyer personas, except social media platforms, there was a consensus around the need for coordination across API security, cybersecurity, and content security strategies. API security is most effective when coordinated with broader content security efforts, but even then, improvements can still be made.

Figure 16: Coordination between API security and cybersecurity strategies

Which best characterizes the level of coordination between your organization's API and cybersecurity strategies?



Note: n=160

© 2025 Omdia

Source: Omdia

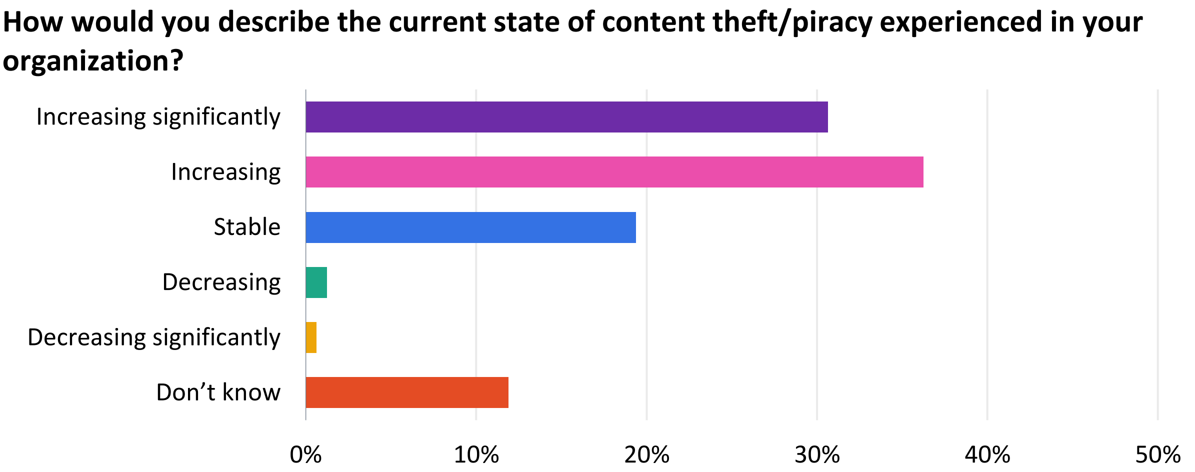
Several factors may have contributed to the differences in coordination level among buyer types:

- OTT service providers are most likely to have high coordination between API security and content security because of streaming platforms' use of horizontally applicable cybersecurity applications that require close coordination among content security areas such as digital rights management (DRM) and watermarking.

- Broadcasters and pay TV operators tend to rely on siloed content security tools separate from cybersecurity applications. However, a large proportion of these two buyer types still reported partial coordination between their API and cybersecurity strategies.

- Not having proprietary content, social media platforms often take a laissez-faire approach to securing content and rely primarily on cybersecurity-related applications to protect their infrastructure.

Figure 17: Piracy is increasing



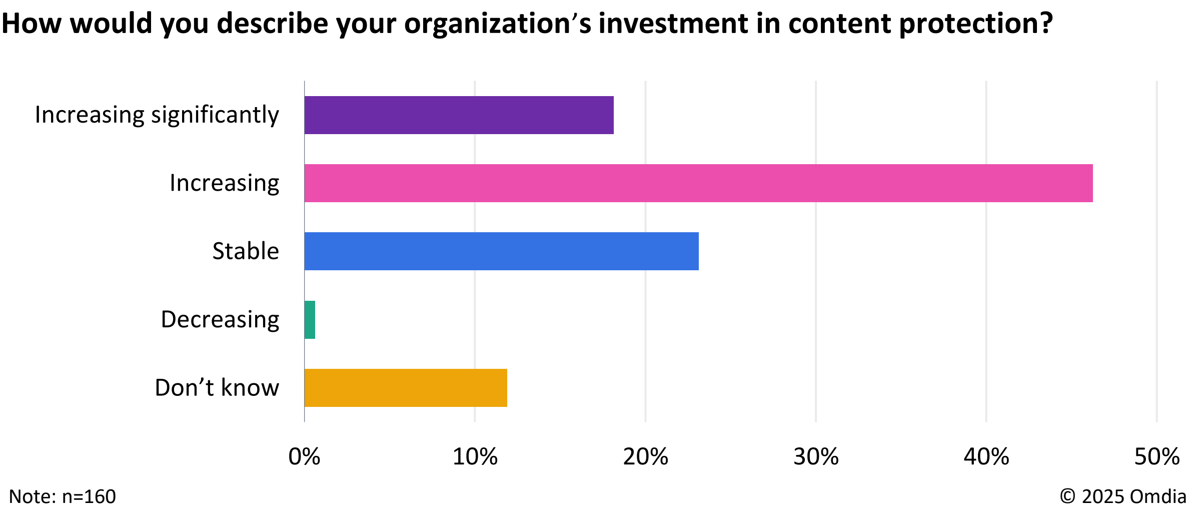
Note: n=160

© 2025 Omdia

Source: Omdia

The threat landscape is alive and ever evolving, and content providers understand that piracy and other abusive practices are growing in intensity, which also involves a widening attack surface. As content providers migrate to IP native distribution architectures, every point in the chain can be accessed by malicious actors. For this reason, encrypting the STB and on-premises hardware within broadcast centers is not a sufficient prevention measure when workflows are rendering deployments marginal to video operations.

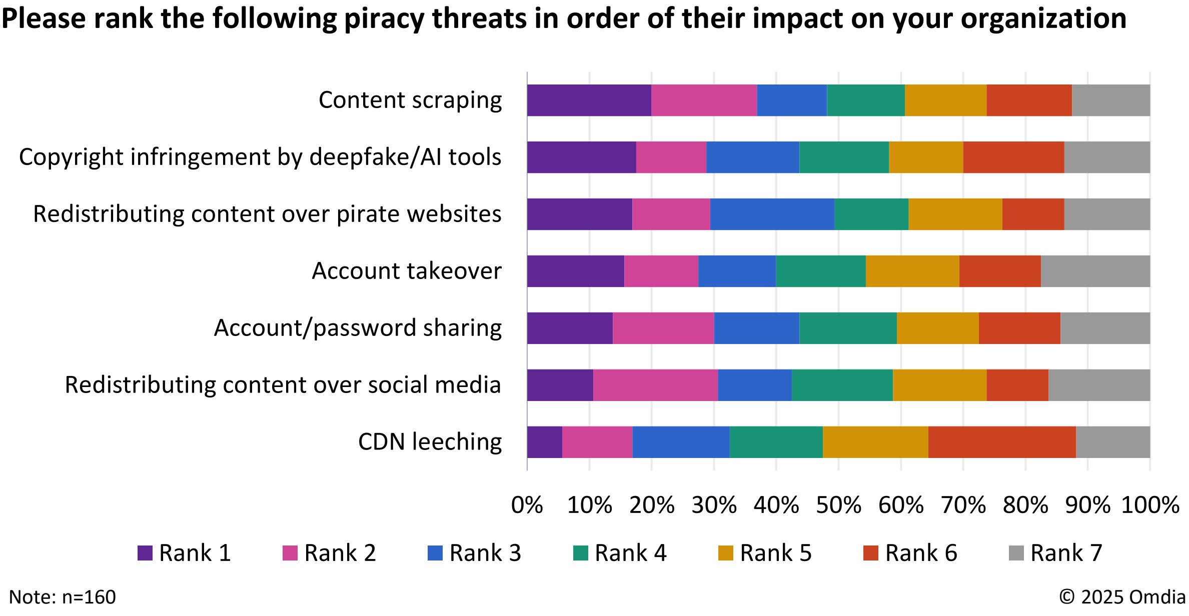
Figure 18: Content protection investment lags threat perception



Source: Omdia

Similarly, premium content providers are responding to heightened threat levels by increasing their investment in content protection. However, this investment falls behind threat perception. VSPs are clearly struggling to match their understanding of the threat landscape with their ability to invest in proactive measures to safeguard their workflows. Though this is entirely natural, this gap between perception and investment is why VSPs require wide-ranging solutions that can blend best practices from cybersecurity, such as API security solutions, with content-specific protection measures.

Figure 19: Piracy threats' effects on organizations



Source: Omdia

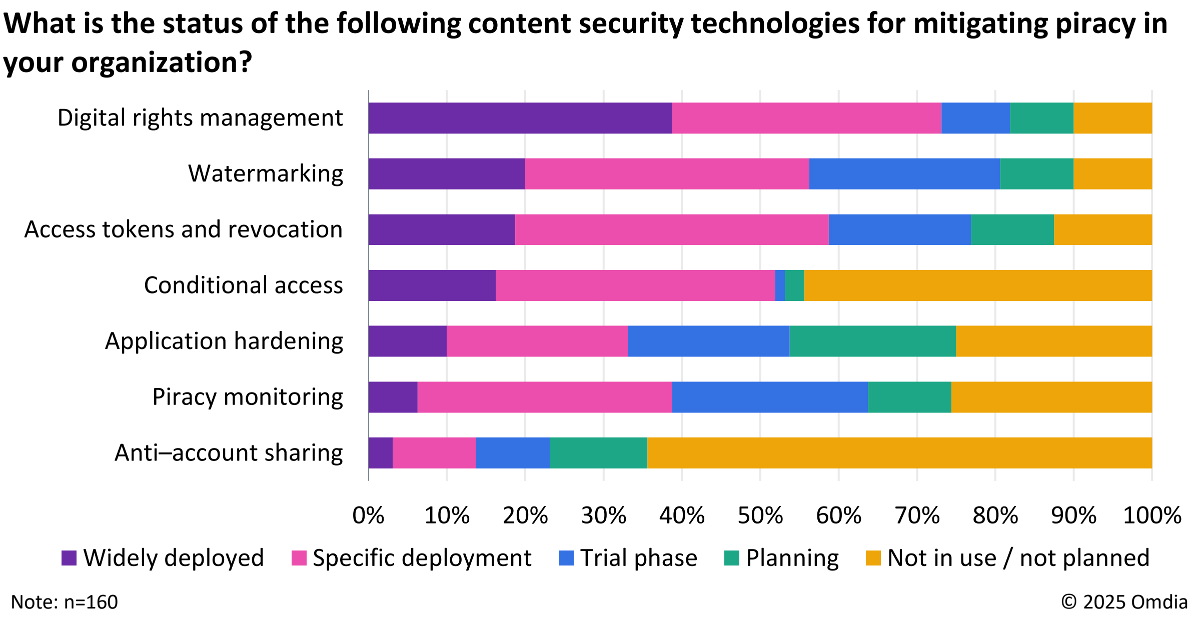
Video services indicated that they face a wide variety of content security threats. However, these threats can be tackled through an approach combining cybersecurity and content security.

Broadcasters and pay TV operators were primarily concerned about content scraping and copyright infringement by deepfake/AI tools and by content redistribution over pirate websites.

Unlike traditional pay TV services, OTT services are not tied to individual households. For this reason, OTT services viewed account abuse through password sharing as a distinct threat.

Account abuse must be addressed with an API-driven approach. Monitoring whether multiple users are using the same account requires the kind of holistic analytics that can only be driven by APIs. Such analytics systems can support the decision-making process by identifying account abuse and even cutting off abusive users and attempting to make them legitimate subscribers.

Figure 20: Organizations’ deployment levels for each piracy-mitigating content security strategy



Source: Omdia

Across the content security landscape, there are some critical technologies already widely deployed by premium content providers that will likely not benefit substantially by any increased investment. These are conditional access, DRM, and token authentication/revocation.

Many respondents indicated that watermarking, app hardening, and piracy monitoring were still in the trial and planning phases and could thus benefit from increased investment going forward. These technologies will also require the use of APIs:

- Watermarking will require APIs to assist in tracking assets.
- For app hardening, apps will be an API endpoint for many inputs. Intellectual property and sensitive user data need protection inside the app environment, and the device operating system may be exposed to hackers and malware.
- Piracy monitoring will require web scraping and legwork to identify malicious actors on the open internet; APIs will be crucial to collecting, validating, and dispatching blocking requests to ISPs.

Recommendations

As organizations look to organize their API security efforts, particularly within the context of media workflows, three key areas emerge:

- First and foremost, there must be alignment between security initiatives and the insights and needs of business teams. Each team will have specific needs in terms of partner relationships, timelines, technologies used, compliance and regulatory demands, and more, and security teams are urged to craft an API security approach that is not only effective but flexible enough to accommodate these diverse needs. As mentioned above, a dedicated API security team may be suitable for facilitating the implementation of an API security strategy, tooling, and operations.

- From a technology perspective, the API security initiative should cover many aspects of the API lifecycle, including discovery, security testing, runtime protection, posture management, and ongoing monitoring. This applies across both APIs being created by the organization and external APIs that are used in support of media workflows. API discovery is critical to identify new, potentially unsafe instances of APIs or data flows within the organization. Security testing is then used to improve the robustness of the implementation against possible threats. Runtime protection and monitoring are essential to maintain a secure state under ongoing operations and to respond to incidents in a timely manner.

- Finally, there is the need to implement API security without disrupting productivity. This will require tight integration between security and business teams to understand needs, but particular attention will need to be paid to inserting API security functionality with minimal disruption. Organizations may choose a phased approach with a focus on awareness and visibility early on, followed by more defined policies as the project matures.

Conclusions and next steps

As this study has shown, API usage within organizations is seeing significant growth in use cases across the media workflow and individual instances of APIs within an IT estate. This growth means securing APIs is becoming a more significant requirement for organizations, from a business perspective (API security as a regulatory or contractual need) and for risk management purposes, since APIs are a highly desirable attack surface for malicious actors.

Moving forward in API security will require organizations to tackle this as a combined business and technology initiative with the right combination of:

- Interaction between teams
- Efficient processes that handle multiple use cases
- An underlying technology foundation that is effective and efficient for the many API security needs, from design through ongoing monitoring

API security should not be separated from the broader content security conversation. APIs are critical to how content is handled across the media workflow, from content capture through distribution and streaming, and a holistic approach is needed to tackle API security across this vast landscape.

As organizations continue to embrace more sophisticated media workflows, securing them with a strong API security program becomes of strategic importance.

Appendix

Methodology

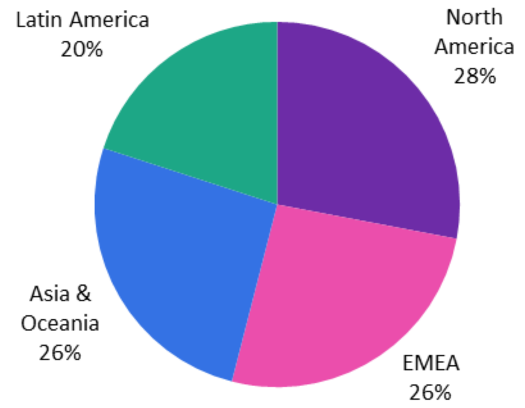
The data for this research comes from a survey fielded by Omdia using a web interface to capture user responses. The survey targeted specific user populations and used extensive validation of results. The summer 2024 survey was fielded online only through a double-blind methodology to ensure that respondents did not know they were taking part in Omdia/Akamai research and that Omdia did not receive any personally identifiable information from respondents.

The survey focused on considerations about how organizations are looking into API security and content security. There were 160 respondents. The criteria for inclusion in the survey included:

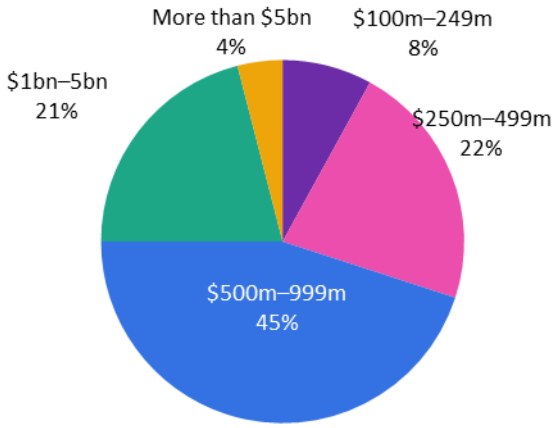
- Specific countries to achieve regional distribution between:
  - North America: the United States, Canada, and Mexico
  - Asia and Oceania: Japan, China, Australia, Indonesia, and India
  - Europe, the Middle East, and Africa: the United Kingdom, Germany, France, the Netherlands, Italy, Spain, Switzerland, and Sweden
  - Latin America: Brazil, Colombia, and Chile
- Businesses in the video services market:
  - Broadcasters
  - Streaming or OTT services
  - Pay TV operators
  - Social media platforms
- Minimum revenue requirements in line with profiles of companies in video services
- Job roles in management or senior management, namely those with influence on decisions related to content protection, fraud, anti-piracy, and API usage

Demographics of participating organizations

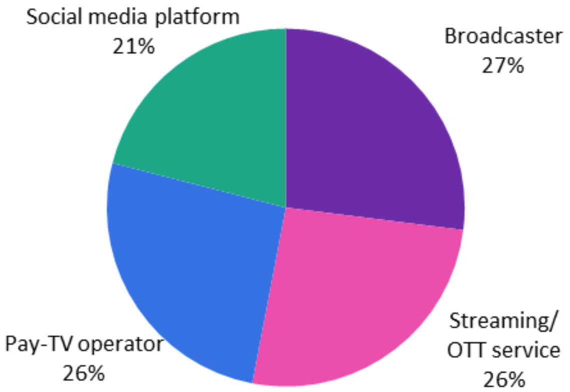
In which region is your organization located?



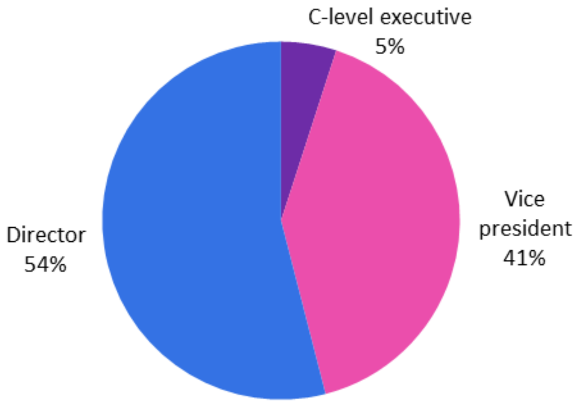
What is your organization’s annual revenue?



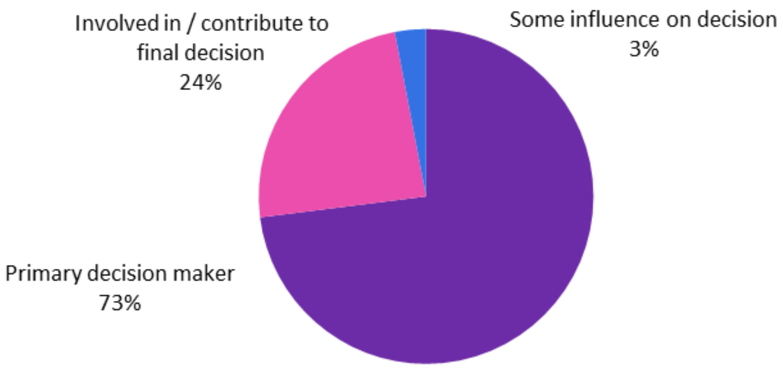
Which best describes your organization with respect to its video services?



Which best describes your job role?



Which best describes your role in making decisions about content protection, fraud, anti-piracy, and API usage for your organization?



Source: Omdia

Authors

Fernando Montenegro
Senior Principal Analyst, Cybersecurity
askananalyst@omdia.com

Thomas Thomson
Senior Analyst, Video Technology
askananalyst@omdia.com

Rik Turner
Senior Principal Analyst, Cybersecurity
askananalyst@omdia.com

Get in touch

www.omdia.com
askananalyst@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 TechTarget, 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.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget 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 TechTarget 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 TechTarget 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 TechTarget 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.