Publication date:
November 2024

Authors:
Christoforos Sarantopoulos
James Crawshaw

Future-Proofing Traffic Management

... with deep network intelligence

OMDIA
Brought to you by Informa Tech

Commissioned by:
allot
See. Control. Secure.

Contents

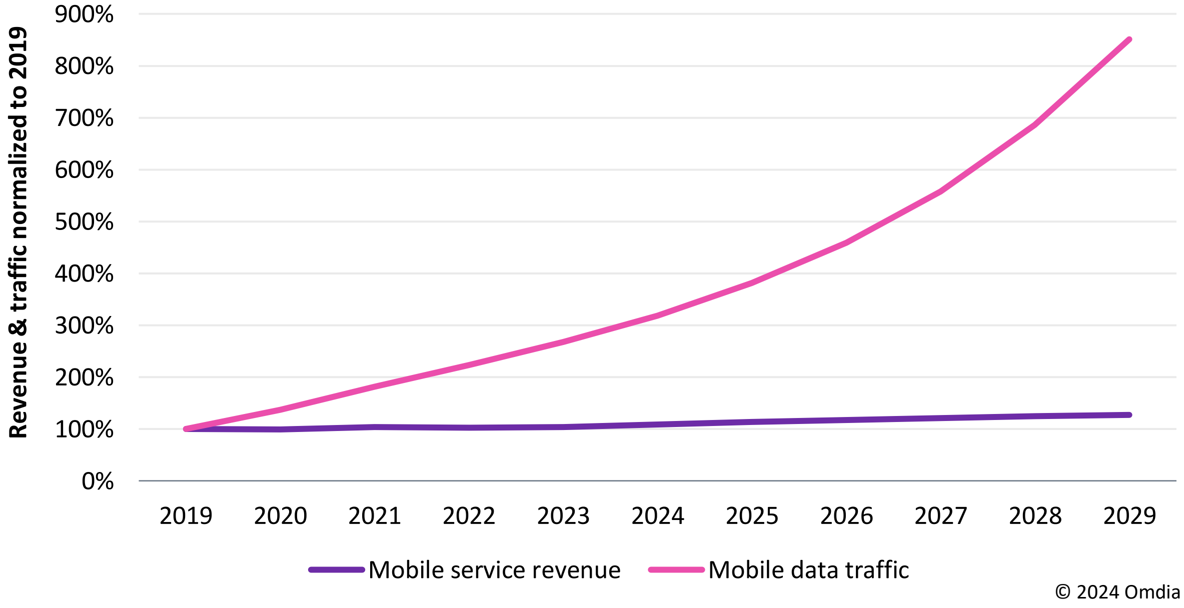
Introduction

The telecom industry is under pressure. For several years, communications service providers (CSPs) have failed to translate the increasing demand for connectivity and communication into sustainable revenue growth. As the data behind **Figure 1** shows, Omdia estimates that global mobile data traffic grew at a CAGR of 28% from 2019 to 2023, while service revenue grew at a CAGR of just 1%. Omdia projects that from 2023 to 2029, traffic will decelerate to a CAGR of 21%, and service revenue CAGR will accelerate to 4%. Nonetheless, the gap between the two growth rates remains large.

Despite a somewhat slower rate of traffic growth, the demand for new services and improved experience is forcing CSPs to continue to invest heavily in their networks. At the same time, an increase in network complexity (disaggregation, virtualization, cloud native) is driving a rise in opex. This is particularly acute in mobile networks with the advent of 5G standalone and the cloudification of core network functions. Managing next-generation networks requires new skills (e.g., Kubernetes) that have not traditionally been present in telco networking teams.

At the same time, CSPs are facing threats from increasingly sophisticated cyberattacks. Security is a critical concern for telcos: network vulnerabilities can be exploited to target not only consumers and enterprises but also governments. In an age of cyberwarfare, it is not just the telcos that are at risk from cyberattacks but the entire digital ecosystem.

Figure 1: Global mobile service revenue has not kept pace with growth in data traffic



Source: Omdia

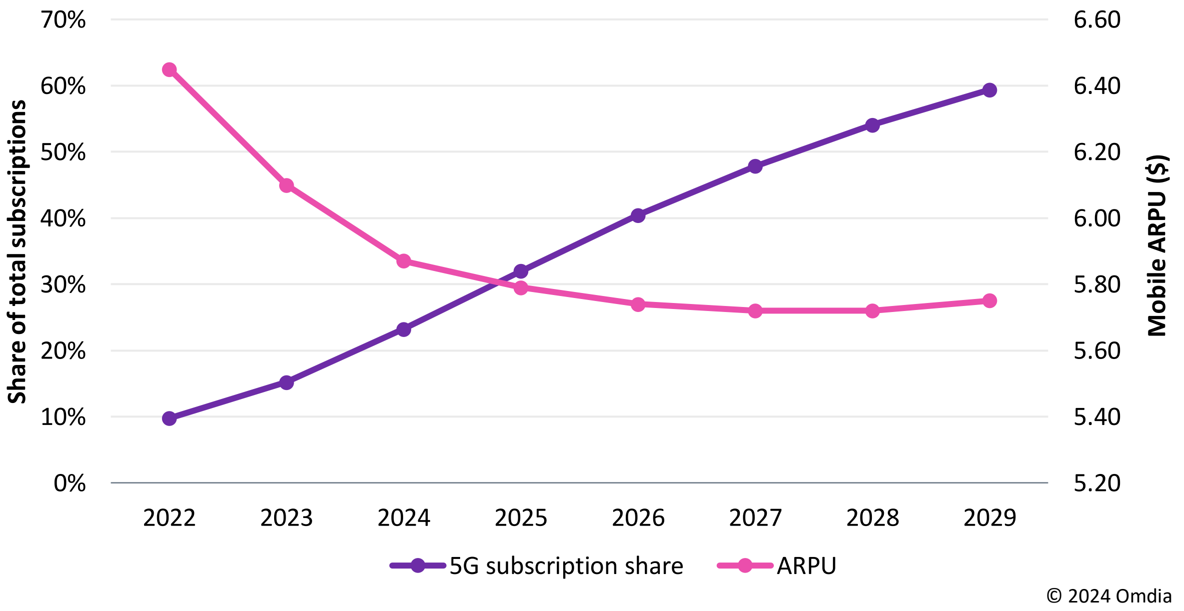
Telcos face increasing business and operational challenges

Revenue growth has stalled

Most CSPs have historically relied on their consumer customers as their primary source of revenue. However, the revenue from consumer services has plateaued in recent years. In developed markets in particular, the introduction of unlimited data and voice plans has crippled CSPs' ability to grow these revenue streams. In the past, consumers paid for voice minutes and data usage, creating a clear path for CSPs to increase revenue as customers used more services, but the shift to flat-rate, all-you-can-eat data plans has commoditized connectivity. In this environment, it is difficult for CSPs to differentiate themselves and extract more value from their customers.

So far, 5G has not delivered on the promise of increased revenue. According to Omdia research, global mobile ARPU is expected to drop by around 5.7% from 2023 to 2029, as shown in **Figure 2**.

Figure 2: Global 5G subscription penetration and mobile ARPU, 2022–29



Source: Omdia

The launch of 5G has had little or no impact on mobile ARPU. Service providers have made significant investments in network equipment and spectrum but have so far failed to monetize them. A lack of content and services that can only be consumed through 5G is one reason for this: for most consumers, 4G is good enough.

In an environment of fierce competition, where data and voice services are increasingly seen as utilities, CSPs must differentiate their offering if they are to outperform their rivals. One possibility is application-based charging, for example, premium quality of experience (QoE) for gaming, streaming, or virtual reality. With these applications, latency and throughput can be critical, which provides an opportunity to upsell. Similarly, CSPs can package new enterprise offerings such as highly secure connections or traffic prioritization for mission-critical applications.

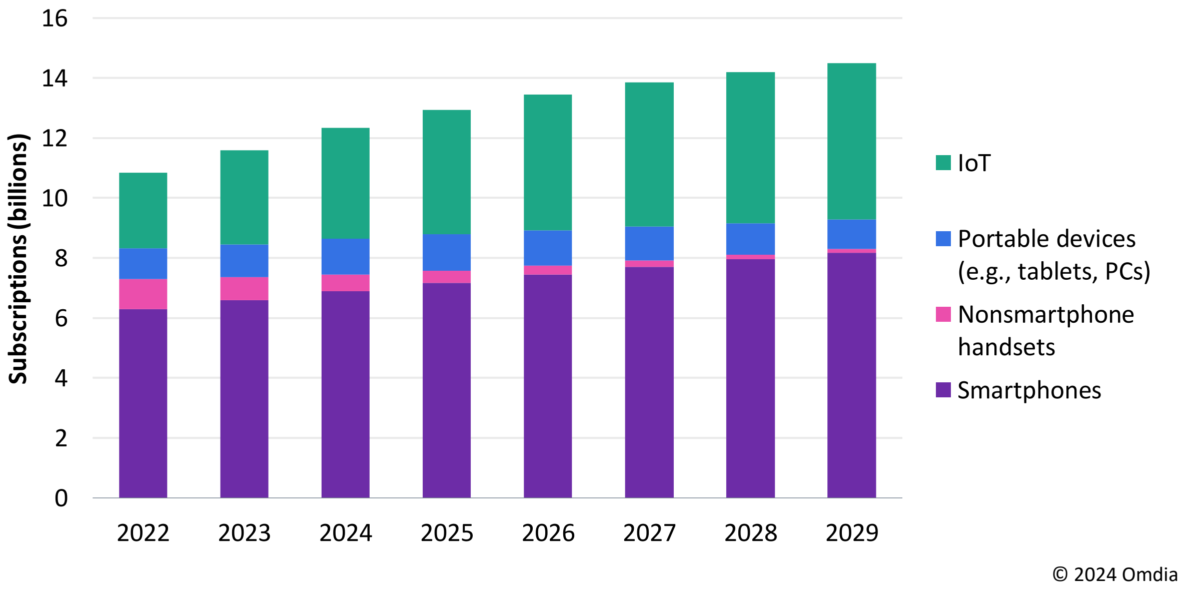
Protecting revenue is a big issue for service providers. Unlimited data plans pose a threat in cases of tethering-data abuse. It is important that CSPs detect fraudulent attempts to bypass fair usage quotas and avoid payment for data consumption.

QoE is increasingly hard to deliver

One of the most pressing challenges for the telecom sector is to define and ensure a suitable and consistent QoE for users based on their individual needs and those of the applications they use.

The increase in the number of connected devices, driven mainly by the Internet of Things (IoT), adds complexity to telecom networks and can make maintaining a consistent QoE a challenge. Omdia forecasts that global mobile subscriptions (including IoT) will increase by 23% between 2023 and 2028 (see **Figure 3**).

Figure 3: Total mobile subscriptions forecast, 2020–29



Source: Omdia

At the same time, new bandwidth-hogging applications are continually being introduced. Immersive gaming platforms and virtual-reality applications could dominate network traffic in the future as high-definition video streaming already does. These data-hungry applications are consuming more bandwidth than ever before, and critical services and users may be left struggling with degraded performance that does not meet their data rate or latency requirements.

CSPs must find a way to allocate network resources so they can support critical or sensitive apps (video streaming, video calls, cloud gaming, business apps, etc.) without compromising the experience of ordinary users. To achieve this, CSPs need more granular visibility into their networks with better control and protection than they have today. Applications with different QoE requirements need to be handled differently by the network. For example, applications such as VoIP and videoconferencing have low overall throughput but high sensitivity to jitter and delay, whereas video streaming requires high throughput but has less or no sensitivity to jitter and delay. Granular visibility also helps in network troubleshooting use cases, helping to identify the root cause of existing issues or to predict issues that may arise by analyzing network traffic.

The increasing prevalence of encryption and obfuscation technologies magnifies this issue. Aside from email, the internet's killer application is the World Wide Web. The key protocol underpinning the web was hypertext transfer protocol (HTTP). However, in the last decade, HTTP has largely been replaced by its more secure version, HTTPS. According to Google's transparency report, [1] 95% of internet traffic is encrypted and carried as HTTPS. HTTP allowed CSPs to analyze and manage data flows relatively easily. However, the shift to HTTPS has limited operators' ability to analyze this traffic. More recently, protocols such as QUIC have been introduced, further hindering network traffic visibility. QUIC is a transport layer protocol used by Google and YouTube (among others) to increase speed and security.

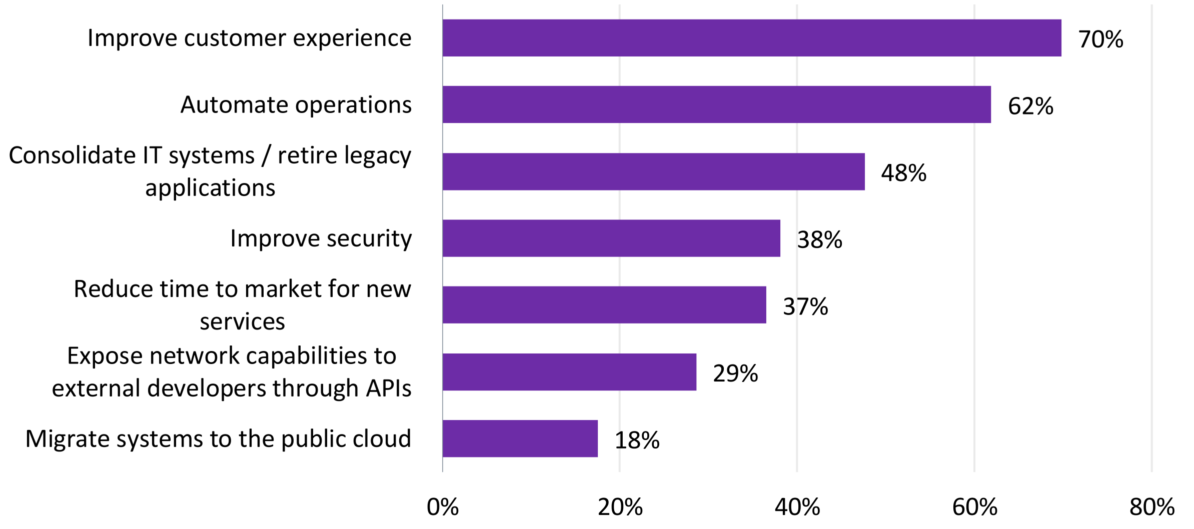
Another future obstacle for traffic visibility is the expected adoption of Encrypted Client Hello (ECH), a security extension protocol in TLS 1.3 (Transport Layer Security) that encrypts the initial "Client Hello" message exchanged between a client and server during connection setup. By encrypting this message, ECH conceals sensitive information from network intermediaries, something that strengthens user privacy. However, this encryption is making it challenging for CSPs to identify and classify traffic accurately. From a more futuristic perspective, post-quantum cryptography (PQC) implementations (algorithms that are secure against attacks from quantum computers) present another riddle to crack for traffic visibility and control systems. Quantum-safe encryption technologies could present additional challenges because service providers need to make sure that all applications and network elements in their environments are ready for PQC.

Encrypting and obfuscating network traffic is a standard method of ensuring security and privacy. As these protocols become more widely used, they will significantly hinder traffic visibility, limiting CSPs' ability to perform detailed traffic analysis, safeguard customer experience, and enforce application-specific policies. Ultimately, without adequate visibility, CSPs will struggle to maintain service quality and optimize traffic management in real time.

[1] Google, "HTTPS encryption on the web," Google Transparency report, available at https://transparencyreport.google.com/https/overview, retrieved November 2024

According to Omdia's research, improving customer experience is a top priority for service providers (see **Figure 4**). Obscuring much of the traffic through encryption significantly limits CSPs' ability to inspect it and guarantee customer experience levels.

Figure 4: Top telco IT priorities



Note: N=63

© 2024 Omdia

Source: Omdia

The growing cybersecurity threat

Cybersecurity is an increasingly important cost for CSPs. Next-generation networks are complex and disaggregated and present an increased attack surface for cyberattacks. Distributed denial-of-service (DDoS) and other forms of cyberthreats are becoming ever more sophisticated. Successful attacks can result in significant harm to a CSP's reputation and, through regulatory fines, its bank balance. At the network level, attacks can significantly increase traffic and further overload the already stressed network infrastructure.

Omdia research indicates that most large-scale DDoS prevention vendors continue to report increases in the number of DDoS incidents of different types, from traditional volumetric attacks to application-level DDoS campaigns. DDoS attacks commonly present threats and consequences in numerous scenarios, including extortion, protests, and political advocacy; individual or team disputes; or the pursuit of geopolitical ends. The increasing use of AI in the automation of the attacks ("AI driven" attacks) amplifies the threat.

The digital transformation of industries makes CSPs responsible not just for providing reliable connectivity but also for making it highly secure. Today, most companies depend on the cloud to run their business. They are looking to CSPs as critical partners in their cybersecurity efforts. For example, BT recently reported that it logs 200 million signals of potential cyberattacks each day.[2] Web-connected devices are scanned over 1,000 times a day on average by known malicious sources such as hackers looking for weaknesses in the online systems of businesses and public services. Criminals are increasingly using “one-time use” disposable bots to evade existing blocking and security measures.

The UK’s National Cyber Security Centre has said that AI will “almost certainly increase the volume and heighten the impact” of cyberattacks over the next two years, [3] and cybercriminals are increasingly using AI to conduct their reconnaissance and carry out more sophisticated attacks.

The elevated responsibility that CSPs face as security guardians for their consumer and business customers creates the need for substantial investment in security tools, and this, if not planned in a smart way, threatens to drive up costs. According to credit ratings agency Moody’s,[4] telecom businesses increased spending on cybersecurity by more than 250% between 2018 and 2023 (a CAGR of 27%), well ahead of the global average across all industries of 100% (15% CAGR). Cybersecurity spending accounted for 10% of the average company’s technology budget in 2023, according to the survey-based report.

[2] BT Group Newsroom (September 12, 2024) “BT spots 2,000 signals of potential cyber attacks every second,” BT, available at https://newsroom.bt.com/bt-spots-2000-signals-of-potential-cyber-attacks-every-second-as-tvs-hunted-star-warns-of-ai-arms-race/

[3] NCSC, (January 24, 2024) “The near-term impact of AI on the cyber threat,” available at www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

[4] Cybersecurity Dive (June 7, 2024) Telecom, media and tech companies are cyber defense standouts: Moody’s,” available at www.cybersecuritydive.com/news/tmt-sector-defense-standouts/718380/

How deep network intelligence can help

Traditional network management tools cannot support the increasingly complex operational environment in which CSPs now find themselves. Telcos need more comprehensive solutions that can provide granular visibility into network traffic, optimize bandwidth allocation through application-aware traffic management, and enhance security. Deep network intelligence (DNI)—smart network management powered by full visibility, analytics, control, and network protection—can help CSPs improve QoE, maximize resource utilization, and implement zero-touch security.

Actionable traffic visibility

As discussed earlier, one of the key challenges CSPs face is gaining complete network visibility, especially as traffic is encrypted today, by protocols such as HTTPS and QUIC, and further obscured in the future, through full encryption (ECH). There is also a need for state-of-the-art PQC support. DNI is a critical component of any network intelligence solution, enabling CSPs to look beyond basic header information and analyze traffic flows. DNI enables the detection of granular traffic patterns, helping CSPs understand not just which applications are being used but also what impact they have on network performance and user experience.

Network traffic visibility can enable CSPs to maintain subscriber awareness, providing insights into how individual users consume network resources. With this awareness, CSPs can tailor services to different user segments, offering personalized QoE optimization based on specific needs or consumption patterns.

For example, enterprise customers might prioritize high-quality videoconferencing and require low-latency connections, while residential users might have varying needs based on their streaming or gaming habits. Subscriber-aware network management allows CSPs to ensure that customers receive the correct QoE / agreed service level with their tiered service plan, thereby enhancing customer satisfaction and loyalty.

Identifying subscriber interests, QoE, and usage patterns enables service providers to introduce targeted promotions that can enable new revenue-generating opportunities. **Table 1** outlines the benefits of traffic visibility.

Table 1: Benefits of traffic visibility

Benefit	Description
Customer usage segmentation	The ability to identify subscriber interests, QoE, and usage patterns enables service providers to introduce targeted promotions.
Detect performance/quality issues	Measure, and understand in detail, factors such as time, location, and device that influence performance issues related to the end users' quality of service and experience.
Plan capacity expansion	Leverage congestion visibility to optimize network expansion to fit current and projected needs exactly, avoiding unnecessary capex and opex.
Identify high-risk churners	Proactively combat churn by identifying at-risk customers based on a combination of factors such as poor QoE and reduced activity.
Analytics as a service for enterprise	Provide enterprise customers with detailed visibility into business-critical service performance issues.

Source: Omdia

Granular, application-aware control

Data-heavy applications have created significant network congestion challenges for CSPs. Traditional traffic management techniques that treat all traffic equally often result in poor performance for critical services (e.g., voice) that are sensitive to jitter and delay when throughput-hungry applications without such requirements (e.g., video streaming) dominate the network.

CSPs need to implement a different type of traffic and congestion management, based on QoE requirements. This should allow them to prioritize traffic dynamically based on application type and user requirements, thereby ensuring optimal service for latency-sensitive and high-priority applications.

Application-aware traffic management can help analyze traffic patterns in real time and make automated adjustments to prevent network congestion from degrading QoE. By recognizing which applications consume the most bandwidth and which users require premium services, CSPs can implement dynamic traffic controls that adapt to changing network conditions. For instance, during peak hours, video-streaming services could be allocated lower priority than real-time applications such as videoconferencing or online gaming, which require low latency and so cannot be buffered or shaped because this would have a great impact on QoE.

Steering traffic based on Layer 7 (Application layer) data can enable more fine-grained traffic management, for example, by routing specific application traffic through value-added services (VAS) solutions. This targeted integration ensures that only relevant traffic is processed by each VAS, optimizing performance and reducing unnecessary load.

Table 2: Intelligent traffic management use cases

Use case	Description
QoE-based congestion management	Ability to provide persistent QoE per subscriber or policy element despite traffic congestion
Layer 7 steering for VAS integration	Ability to steer traffic per application
Traffic prioritization	Ability to provide traffic prioritization and, as a result, to maintain required subscriber QoE during periods of congestion

Source: Omdia

Supporting new service monetization

Beyond optimizing the network performance with more visibility into network traffic, DNI can offer CSPs a way to access new revenue. In an era of flat-rate and unlimited data plans, CSPs must move beyond traditional revenue models. Network intelligence solutions allow CSPs to tap into innovative monetization strategies by providing the tools needed to deliver premium, differentiated services.

DNI solutions can interface with charging and provisioning systems, enabling the rapid rollout of differentiated services based on the needs of consumers and enterprise customers. At the same time, identifying applications at Layer 7 of the inspected packet data can enable application-based charging.

Furthermore, CSPs can monetize tethering and block fraudulent traffic. The main monetization use cases are presented in **Table 3**.

Table 3: Service monetization use cases

Use case	Description
Rapidly deploy differentiated services	Cater to the unique and dynamic needs of prepaid, postpaid, business, and IoT customers via seamless integration to provisioning and charging systems.
Application- or volume-based charging	Precise identification of applications at Layer 7 allows CSPs to differentiate their offering based on targeted service bundles. Granular metering enables volume-based charging.
HTTP header enrichment	Leverage customer information to improve and personalize their online experiences by forwarding anonymized customer information to over-the-top and content provider websites.
Monetize or block tethering	Block or upsell tethering to drive/protect revenue by preventing abuse of mobile broadband.
Detect fraudulent data traffic	Identify fraudulent data usage that attempts to bypass usage quotas and avoid payment for data consumption.

Source: Omdia

A solution with these features would enable CSPs to quickly roll out attractive, differentiated services. A differentiated services offering (e.g., tiered plans) could strengthen customer choice and increase loyalty. It could also help increase revenue by upselling to either high-data users or tethering users. Finally, it could help protect revenue by providing more accurate metering and charging, blocking fraudulent traffic, and stopping tethering abuse.

Enabling regulatory compliance

The ability to detect granular traffic, identify specific types of traffic (voice, video, etc.), and distinguish between legitimate and potentially harmful or prohibited applications enables CSPs to classify traffic, enhancing service differentiation and the implementation of precise service-related policies.

Policy enforcement is also essential for CSPs, whose networks are deemed infrastructure of national importance, to comply with government regulations. Governments worldwide impose strict rules on content regulation and blocking dangerous applications. CSPs need solutions that enable them to adhere to these regulations without compromising network performance. Deep network intelligence allows CSPs to implement filtering, content blocking, and traffic monitoring mechanisms that comply with national and international regulations.

Enhancing security against sophisticated threats

Finally, a DNI framework should provide network security, enabling networks to autonomously detect and respond to threats in real time.

One of the critical benefits of DNI is its ability to identify anomalous behavior patterns that indicate potential cyber threats, such as DDoS attacks and unauthorized access attempts. Machine learning (ML) models can analyze network traffic and provide dynamic and intelligent firewall implementations.

A DNI solution should encompass security features including the following:

- **Anti-DDoS:** Detection of inbound and outbound volumetric attacks, ML-based zero-day detection, hit-and-run attack identification, automatic mitigation, and traffic scrubbing through dedicated centers

- **Anti-botnet:** Host behavior analysis, threat intelligence to detect C2C communication, and automatic isolation of compromised devices or subscribers

- **Network firewall (FW):** Access control, DNN- and slice-specific allow/block lists, and content filtering to regulate and secure network access

- **QoE protection:** Policy-driven application prioritization to ensure QoE, DPI-based application detection, and protection of communication link capacity, critical infrastructure, and protocols

- **Visibility and analytics:** Performance impact analysis for network services and critical applications along with detailed forensic capabilities for threat and attacker analysis

Conclusions

To survive in the 21st century, telecom operators must improve their operational efficiency and find a way to safeguard their offered QoE in challenging conditions. To do so, CSPs need to transform their networks from simple data carriers to smart systems capable of addressing a range of business, operational, and security challenges. The solution to many of the challenges they face lies in the adoption of deep network intelligence, which can provide

- Smart and granular app-aware traffic management, even for encrypted flows
- QoE estimation for video streaming and gaming services
- Identification of network congestion to apply appropriate policies
- Enhanced security (e.g., protection against DDoS attacks and botnets)
- Fairness and prioritization of network traffic
- Enablement of new business models (e.g., application-based charging)

DNI provides the essential tools to understand the causes of poor service and network performance. It helps CSPs to optimize their networks in real time and make sure that bandwidth-hungry applications do not overshadow more critical services.

As CSPs prepare for a new age of telco services underpinned by 5G, fiber to the home, and edge computing, DNI will be a key enabler in driving efficiency, customer satisfaction, and growth.

About Allot

This section is written by Allot

Allot is a leading provider of innovative network intelligence and security solutions that empower CSPs and enterprises worldwide to enhance the value they bring to their customers. With over 20 years of proven success, our solutions turn network, application, usage and security data into actionable intelligence that make our customers' networks smarter and their users more secure.

Our Allot Smart solution suite, powered by inline Deep Network Intelligence (DNI) technology, generates insightful intelligence that empowers our customers to optimize, innovate, and capitalize on every service opportunity. By analyzing every packet of network, user, application and security data, Allot Smart cost-effectively enables the highest Quality of Experience (QoE) for our customers' end-users. Using Allot Smart, our customers have lowered access bandwidth costs by 10%, deferred capacity expansions by 1-2 years and reduced revenue leakage by 15%.

Allot's multi-service platforms are deployed globally, in the most demanding environments, by over 500 mobile, fixed and converged service providers and over a thousand enterprises. We support evolving network architectures by offering the most flexible platforms in the market, including COTS hardware, software only and field-proven, fully NFV compliant solutions.

Allot has been publicly traded on the NASDAQ and Tel Aviv Stock Exchange since 2006 under the ticker symbol ALLT.

Appendix

Author

Christoforos Sarantopoulos
Senior Analyst, Service Provider Transformation
askananalyst@omdia.com

James Crawshaw
Practice Leader, Service Provider Transformation
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 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.

.

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.