

Dipartimento  
di Impresa e Management

Cattedra di Economia e Gestione dei Media

# La contendibilità nel mercato delle Content Delivery Network (CDN). Focus sul contesto italiano.

Prof. Luca Balestrieri

---

RELATORE

Prof. Gianluca Comin

---

CORRELATORE

Lorenzo Costa Matr. 720681

---

CANDIDATO



# INDICE

<b>CAPITOLO 1: SCENARIO DI RIFERIMENTO</b>	<b>7</b>
1.1 LA RETE IP	7
1.2 EFFETTO COVID	9
1.3 LA SOCIETÀ DIGITALE ( <i>GIGABIT SOCIETY</i> ) E LA BANDA ULTRA-LARGA FTTH	12
1.4 <i>TREND</i> DEL TRAFFICO IP E L'EFFETTO VIDEO: PANORAMICA E CRITICITÀ	15
1.5 LA NUOVA SFIDA: LA <i>QUALITY OF EXPERIENCE</i> (QoE)	19
1.6 COME ASSICURARE UNA ELEVATA QoE?	22
1.7 EDGE COMPUTING	27
1.8 PREVISIONI	31
<b>CAPITOLO 2: LE CONTENT DELIVERY NETWORK</b>	<b>35</b>
2.1 UN PO' DI STORIA	35
2.2 L'AVVENTO DI AKAMAI	37
2.3 IL RUOLO STRATEGICO DELLA TELEVISIONE NEL MERCATO DELLE CDN	39
2.4 COME FUNZIONA UNA CDN?	41
2.5 I DIVERSI TIPI DI CDN	46
2.6 VANTAGGI NELL'UTILIZZO DI UNA CDN	47
2.7 LA SFIDA ATTUALE: LE CDN NELLO <i>STREAMING</i>	48
2.8 EVOLUZIONE DEL TRAFFICO SU CDN	51

## **CAPITOLO 3: LA CONTENDIBILITÀ NEL MERCATO ITALIANO** **55**

### **3.1 IL LEADER DEL MERCATO: AKAMAI OVERVIEW** **55**

3.1.1 LA STRATEGIA DI AKAMAI 57

3.1.2 LA TECNOLOGIA E IL NETWORK 58

3.1.3 I PRINCIPALI SERVIZI OFFERTI 58

3.1.4 FOCUS SULLA CDN DI AKAMAI 61

3.1.5 L'AMBIENTE COMPETITIVO 62

3.1.6 I PRINCIPALI RISCHI 63

### **3.2 I COMPETITORS: LO SCENARIO DI RIFERIMENTO** **65**

3.2.1 AMAZON: FATTURATO E RICAVI 69

3.2.2 AMAZON WEB SERVICES 70

3.2.3 INFRASTRUTTURA GLOBALE DI AWS E PRINCIPALI VANTAGGI 71

3.2.4 PRINCIPALI SERVIZI OFFERTI DA AWS 73

3.2.5 CLOUDFRONT PER LO STREAMING VIDEO IN DIRETTA E ON-DEMAND 78

3.2.6 PANORAMICA DI MERCATO DEI CLOUD INFRASTRUCTURE & PLATFORM SERVICES (CIPS) 81

3.2.7 AWS PUNTI DI FORZA E DEBOLEZZA/CRITICITÀ 82

### **3.3 AWS CLOUDFRONT VS AKAMAI CDN** **84**

### **3.4 LIMELIGHT NETWORKS** **87**

### **3.5 FASTLY** **88**

### **3.6 MAINSTREAMING** **90**

### **3.7 CLOUDFLARE** **92**

## **CONCLUSIONI** **97**

## **APPENDICE SULLA SICUREZZA** **100**

## **RINGRAZIAMENTI** **108**

## **BIBLIOGRAFIA E SITOGRAFIA** **109**

## **RIASSUNTO** **113**

# INTRODUZIONE

Stiamo entrando in una nuova fase dello sviluppo economico e sociale, frutto di un continuo e inarrestabile processo di innovazione che ha caratterizzato nel corso degli ultimi due decenni lo sviluppo di Internet, favorendo la diffusione della *digital economy* in tutti i settori, non più legati soltanto all'ICT. Questa trasformazione è il risultato dell'evoluzione e dell'espansione di Internet come perno attorno al quale ruota qualsiasi attività; esso incide infatti sia sui modelli di *business*, con effetti rilevanti di *disruption* di particolari settori economici, sia sulle abitudini e stili di vita dell'intera società. In questa rivoluzione tecnologica, come in tutte le precedenti, le infrastrutture sono alla base dello sviluppo economico: le tecnologie abilitanti non potrebbero esistere senza adeguate infrastrutture sottostanti. Pertanto, nella *digital economy*, un presupposto essenziale per una nuova fase di crescita dello sviluppo economico è rappresentato dalla disponibilità di un'infrastruttura di telecomunicazioni a banda ultra-larga estremamente affidabile, *future proof* e con una copertura del 100%.

Internet, nella sua prima fase di sviluppo (*Web 1.0*), era caratterizzato prevalentemente da siti statici, senza alcuna possibilità di interazione con l'utente, eccetto la normale navigazione tra le pagine, l'uso della posta elettronica e le funzioni di ricerca. Oggi, invece, Internet pervade ogni ambito della società (*connected society* e *internet of things*), anche in chiave di offerta di servizi, per cui ogni processo di comprensione delle informazioni viene facilitato dalle macchine, al fine di fornire un'esperienza più produttiva e intuitiva all'utente.

Il traffico su rete IP è cresciuto esponenzialmente negli ultimi anni e il principale *driver* di tale crescita è il video che in tutte le sue forme (*live, on-demand, gaming*) rappresenta circa l'80% di tale traffico. Data la centralità che il video sta assumendo, le varie piattaforme (Netflix, Youtube, Amazon Prime, DAZN) hanno focalizzato il proprio interesse sulla *Quality of Experience (Qoe)* dell'utente. In questo contesto è fondamentale che i consumatori possano fruire dei contenuti *online* con una qualità adeguata: sia chi offre servizi di video *streaming* (OTT), sia chi offre servizi di *web browsing* per sviluppare il proprio *business* ha quindi la necessità di soggetti che si occupino di *delivery* di contenuti e applicazioni. Si sono così sviluppate le *Content Delivery Network (CDN)*.

Proprio l'incapacità dei Telco di rispondere in modo tempestivo al passaggio da una situazione *voice centric* ad uno scenario *data centric* e l'inadeguatezza dei modelli di interconnessione tradizionali (*end-2-end* di tipo "*best effort*") ha favorito l'affermazione di soggetti (es. Akamai, Limelight, CloudFlare) che offrono, a livello globale, servizi di *delivery* di traffico IP. Essi assicurano una qualità migliore di quella ottenibile con un trasporto *end-2-end* di tipo "*best effort*" mediante, ad esempio, soluzioni di *caching, web acceleration, Content Delivery Network*.

Una rete CDN è una piattaforma di *server* altamente distribuita che aiuta a minimizzare il ritardo nel caricamento dei contenuti delle pagine *web*, riducendo la distanza fisica e logica tra il *server* e l'*end-user*, così da assicurare agli utenti in tutto il mondo di visualizzare gli stessi contenuti ad alta qualità senza rallentare i tempi di caricamento. L'obiettivo della rete CDN è quello di incrementare la velocità di un sito *web* riducendo, al contempo, la latenza, ossia il ritardo tra l'inoltro di una richiesta su una pagina *web* ed il completamento del caricamento della pagina sul dispositivo in uso, che si ottiene riducendo la distanza fisica che deve compiere la richiesta.

Gran parte del traffico Internet viene gestito tramite CDN e, entro il 2022, il 72% del traffico sarà trasportato tramite CDN con ampie prospettive di crescita futura. Si tratta infatti di una tecnologia caratterizzata da elevata maturità ed alto valore aziendale.

Questa tecnologia è presente sul mercato da decenni e il nucleo di funzionalità è rimasto sostanzialmente invariato. Le CDN sono e saranno essenziali per offrire un'esperienza di *streaming* video di alta qualità. Akamai Technologies è l'azienda *leader* nel panorama delle CDN, la società fornisce soluzioni per la protezione, la distribuzione e l'ottimizzazione di contenuti e applicazioni aziendali su Internet.

Il presente elaborato mira a stabilire se la posizione che Akamai ha raggiunto nel mercato del *content delivery* dopo 23 anni dalla sua nascita, nel 1998, sia contendibile da altri *player*, sia attuali che potenziali.

La piattaforma di Akamai è in continua crescita e sviluppo; essa rappresenta il vero valore aggiunto e il vero vantaggio competitivo rispetto ai *competitor*. Nel corso degli anni ha consolidato i rapporti di *peering* e ha raggiunto livelli di penetrazione con gli ISP difficilmente raggiungibili. Nell'ultimo decennio nuove realtà come Limelight, Fastly e soprattutto i *big tech* come Amazon, Google e Apple sono entrate in tale *business*, perseguendo una strategia molto aggressiva per conquistare rapidamente quote di mercato e competere con Akamai.

Dopo aver, quindi, analizzato lo scenario di riferimento e il funzionamento delle *Content Delivery Network*, il mio studio si è concentrato sul mercato di queste ultime a partire da un'analisi approfondita del *leader* del mercato: Akamai. Ho poi analizzato l'ambiente competitivo di questo mercato, evidenziando in particolare tre livelli di competizione: Operatori *Big Tech*, Operatori Telefonici e Operatori che si concentrano solo sulla *delivery*. Per condurre questo tipo di analisi, data la scarsità di dati pubblici da cui poter attingere, ho intervistato alcuni dei principali *player* nel mercato come Akamai, Amazon Web Services e Mainstreaming. Attraverso il confronto con tali aziende, ho potuto comprendere più in profondità le dinamiche competitive caratterizzanti il mercato del *content delivery*, la contendibilità del mercato e i possibili scenari futuri.

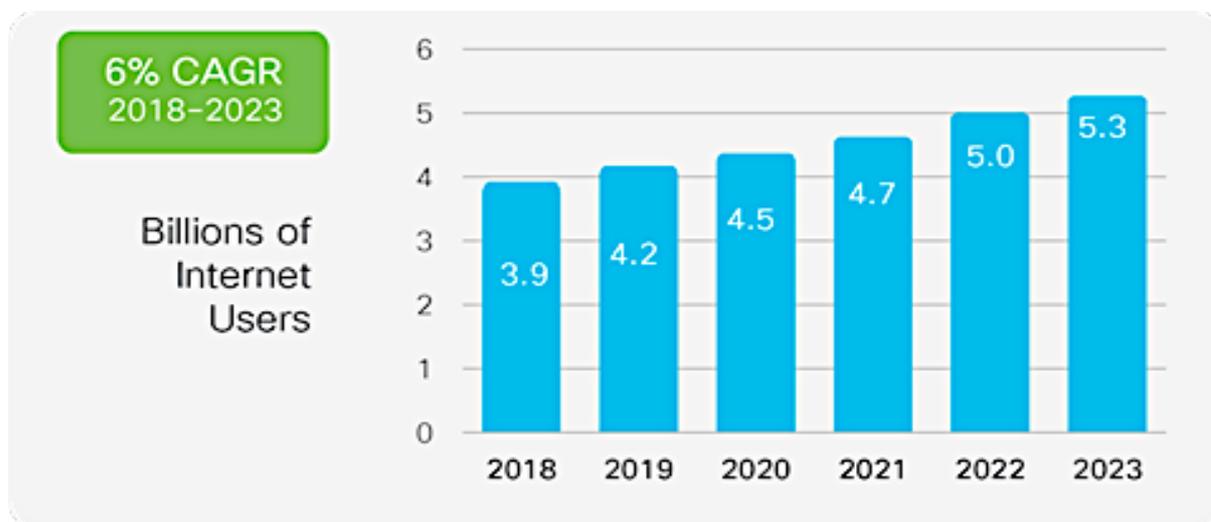
# CAPITOLO 1: SCENARIO DI RIFERIMENTO

## 1.1 La rete IP

Dalla sua introduzione agli inizi degli anni '60, Internet ha completamente cambiato la vita di miliardi di persone. Sulle reti pubbliche e private di cui si compone è transitato un traffico di dati pari a oltre 4,7 Zettabyte. La straordinaria evoluzione di Internet avvenuta negli ultimi due decenni getta le basi per una nuova era caratterizzata dalla digitalizzazione della società, grazie allo sviluppo delle reti a banda ultra-larga che determineranno il raggiungimento di un livello di automazione senza precedenti, attraverso il collegamento alla rete di persone e oggetti. Eppure secondo il nuovo studio Visual Networking Index (VNI) di Cisco<sup>1</sup> questo è solo l'inizio. Entro il 2022, sulle reti globali transiterà più traffico di dati di quanto ne sia passato in tutti gli "anni – Internet" dal 1984 al 2016. In altre parole: nel solo anno 2022 sarà creato più traffico dati di quello creato nei 32 anni (1984-2016) messi insieme<sup>2</sup>.

Da dove arriverà tutto questo traffico dati? Da tutti noi, dalle nostre macchine, dal modo in cui usiamo Internet. *Cloud Computing, Internet of Things, Big Data & Analytics, Blockchain, Advanced robotics e 3D printing e 5G* costituiscono i nuovi strumenti abilitanti della *digital economy* che, grazie alla sua diffusione pervasiva in tutti i settori, promette di dar luogo a una nuova era dello sviluppo economico e sociale. Entro il 2022, il 60% della popolazione mondiale userà Internet [Grafico 1]. Saranno *online* più di 35 miliardi tra *devices* e connessioni.

Grafico 1 - Crescita globale degli utenti Internet.



Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

<sup>1</sup> Cisco Visual Networking Index™ (Cisco VNITM), Cisco.

<sup>2</sup> Saporiti Riccardo, *Quanti sono 4,8 zettabyte? Il traffico dati su Internet tra il 1984 ed il 2016*, 13 dicembre 2018, Il Sole 24 Ore.

La nostra concezione di Internet come risorsa affidabile ed illimitata, tuttavia, sta venendo sempre più messa a dura prova dalla diffusione globale della pandemia *coronavirus*. Le conseguenze della crisi pandemica hanno rappresentato uno straordinario *stress-test* delle infrastrutture critiche del Paese, che mette in luce un duplice aspetto. Da un lato, la tendenza all'utilizzo di processi di elaborazione dei dati nelle vicinanze in cui vengono generati (cosiddetto *edge computing*), rende la rete strettamente dipendente dalla dislocazione e dalla densità dei *server* sul territorio; conseguentemente, quei Paesi che presentano un'infrastruttura non in grado di assicurare lo stesso livello di servizio in tutto il territorio e che hanno un numero limitato di *server* dislocati nel paese, scontano un *gap* tecnologico ed economico circa il buon funzionamento di Internet e rischiano di cedere il passo nella competizione globale.<sup>3</sup>

Dall'altro lato si è reso ancor più evidente come il nostro Paese sia caratterizzato da situazioni infrastrutturali differenziate che fanno emergere diseguaglianze territoriali e impongono riflessioni di politica industriale. In Italia, infatti, è presente una forte discrepanza tra copertura infrastrutturale del territorio e penetrazione dei servizi: a fronte di livelli di copertura territoriale che potenzialmente consentono all'88,9% delle famiglie italiane di accedere a servizi Internet con velocità maggiori o uguali a 30 Mbps, solo il 37,2% di esse possiede effettivamente una simile connessione<sup>4</sup>. Data questa condizione, risulta difficile per gli operatori offrire servizi qualitativamente migliori.

Tale disparità è indubbiamente legata a profonde differenziazioni di tipo geografico. Nelle regioni meridionali, ad esempio, la forbice tra copertura (infrastrutturazione) e diffusione (penetrazione) dei servizi *broadband* e *ultrabroadband* appare assai maggiore. Infatti, nelle regioni che hanno goduto di investimenti infrastrutturali di Stato (come la Sicilia e la Calabria) non si è assistito al successivo decollo dei servizi. Ciò mette ulteriormente in luce quanto l'effettiva penetrazione sia un fenomeno complesso in cui un ruolo chiave è svolto da variabili legate alla domanda. Stimolare la capacità di spesa delle famiglie, quindi, rappresenta uno strumento necessario da affiancare alla pianificazione degli investimenti infrastrutturali, al fine di dare un forte impulso al processo di digitalizzazione del Paese, fondamentale in un periodo di crisi economica come quello attuale.

---

<sup>3</sup>Ad esempio, secondo la ricerca condotta da Tech4i2 (*Coronavirus impact on Internet use*), le infrastrutture di *cloud service* sono significativamente minori nel Sud e nell'Est Europa determinando un rallentamento maggiore in queste zone.

Fonte: <https://bit.ly/3bSDhPC>.

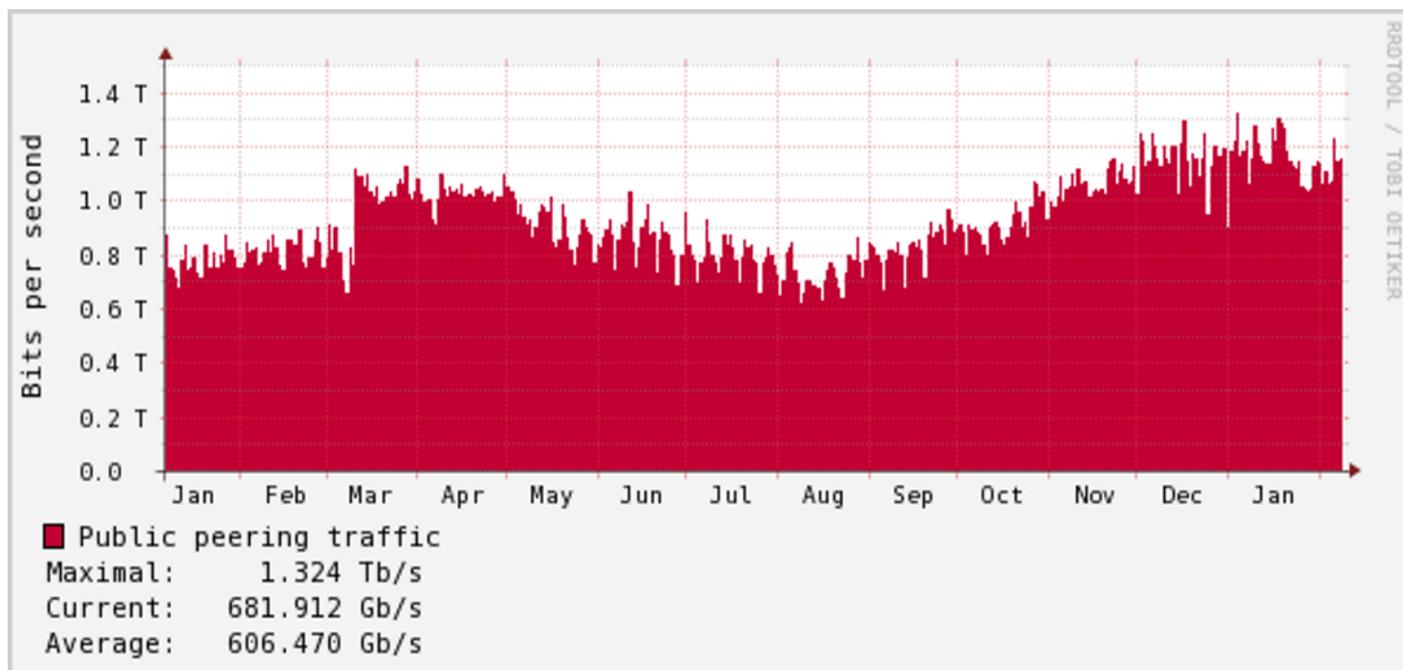
<sup>4</sup> *Relazione annuale*, AGCOM, 2020.

## 1.2 Effetto Covid

Il *lockdown* scaturito a seguito della pandemia da Covid-19 ha reso evidente il ruolo nevralgico svolto dalle reti di comunicazione. Internet è diventato il centro delle attività sociali, ricreative e lavorative. Nella fase di quarantena le reti hanno permesso a milioni di persone di lavorare, studiare, fare acquisti e mantenere i propri contatti sociali nonostante le restrizioni negli spostamenti. La permanenza forzata delle persone nelle proprie abitazioni ha avuto effetti notevoli sul sistema nazionale di telecomunicazione.

Il 2020 ha visto il traffico Internet raggiungere nuove vette, con un *trend* di crescita ormai consolidato. Questo effetto non è legato solo allo *smart working* o alla didattica a distanza. Queste due componenti hanno avuto certo il loro impatto, ma, come testimonia l'impennata del traffico nazionale a fine anno e in particolare durante il periodo delle festività natalizie, a crescere sono soprattutto *gaming* e *streaming*. Il solo MIX di Milano, uno dei più grandi Internet *Exchange* europei per traffico veicolato, ha fatto registrare a dicembre un picco di 1,2 terabit/s, più alto di quello del *lockdown* di marzo 2020, quando si passò dall'oggi al domani da 0,9 terabit/s a oltre 1,1 terabit/s. Da quel momento la crescita è stata costante e a gennaio è già stato raggiunto un nuovo picco superando, sempre considerando solo il MIX, la soglia dei 1,3 terabit/s<sup>5</sup> [Grafico 2].

Grafico 2 - L'andamento del traffico Internet del 2020 riportato dal MIX di Milano.

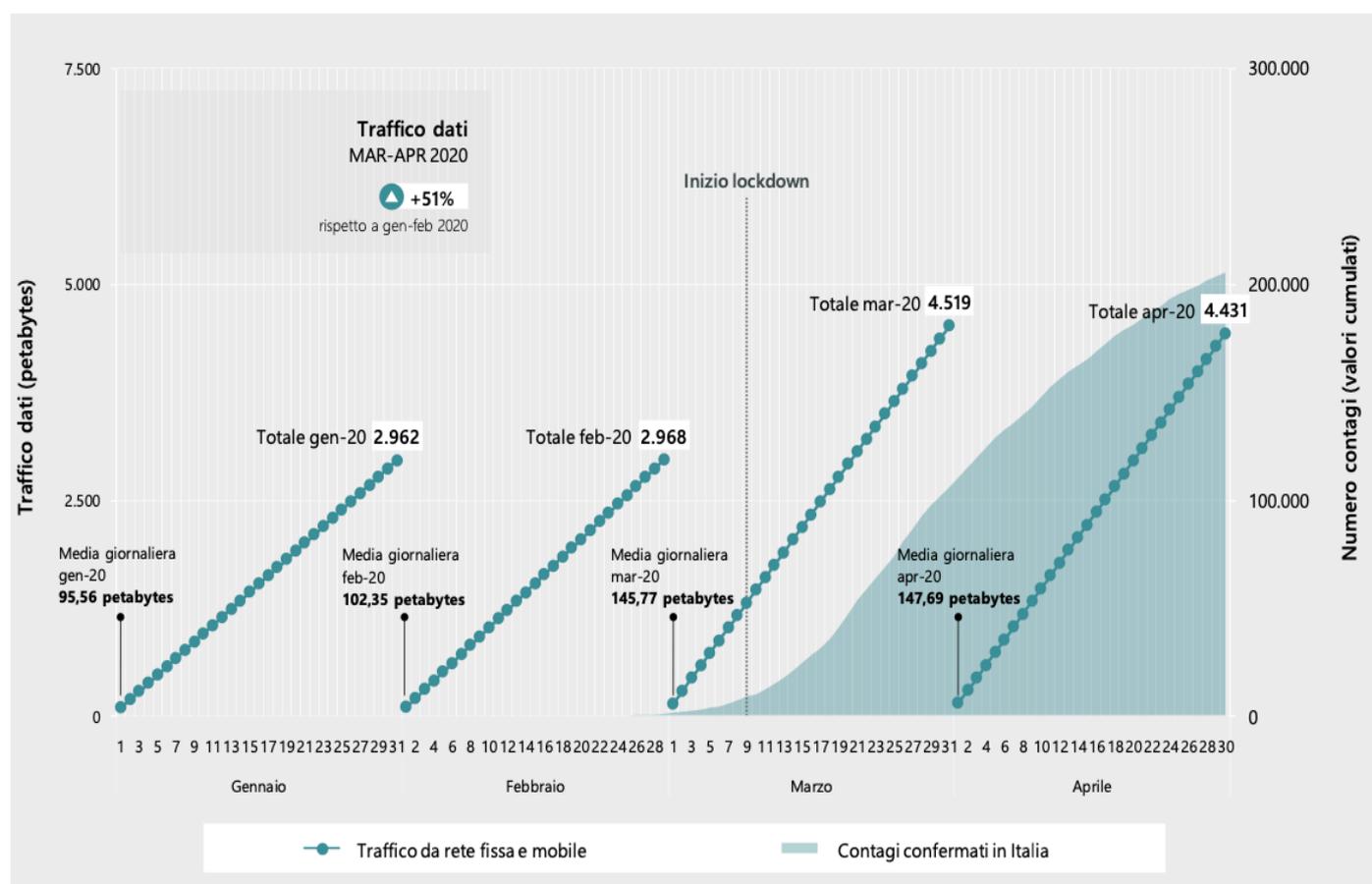


Fonte: MIX di Milano

<sup>5</sup> Akamai: nel 2020 esplosione di streaming e gaming. Una partita di calcio in streaming genera 1 terabit/s di traffico, DDAY, 8 febbraio 2021. Articolo pubblicato su Digital Day.

Durante la prima ondata pandemica, l'Agcom ha effettuato un monitoraggio del traffico sulle reti di telecomunicazione a cui hanno partecipato 24 operatori di rete fissa (pari al 99% del mercato) e 8 operatori di rete mobile (pari al 97% del mercato)<sup>6</sup>. Dall'analisi è emersa chiaramente la correlazione tra l'entrata in vigore delle disposizioni per limitare la mobilità dei cittadini italiani e l'aumento del traffico di rete. Durante il *lockdown* il volume di traffico dati è aumentato del 57% su rete fissa e del 29% su rete mobile rispetto al mese di febbraio 2020. Parimenti il traffico voce ha visto un'impennata del 49% da fisso e del 37% da mobile [Grafico 3]. Con l'inizio della fase 2 e le concomitanti prime riaperture, i valori si sono lievemente ribassati, attestandosi a quota +28% su rete fissa e del +15% su rete mobile rispetto ai numeri pre-emergenza sanitaria. L'incremento nell'utilizzo del traffico dati risulta ancora più evidente se osserviamo i valori medi giornalieri, sia fissi che mobili, di *petabytes* transitati. Il traffico medio giornaliero ha sperimentato una crescita verticale dai 95/100 *petabytes* di gennaio e febbraio ai 147 di marzo e aprile<sup>7</sup>.

Grafico 3 - Traffico su rete fissa e mobile gennaio-aprile 2020.

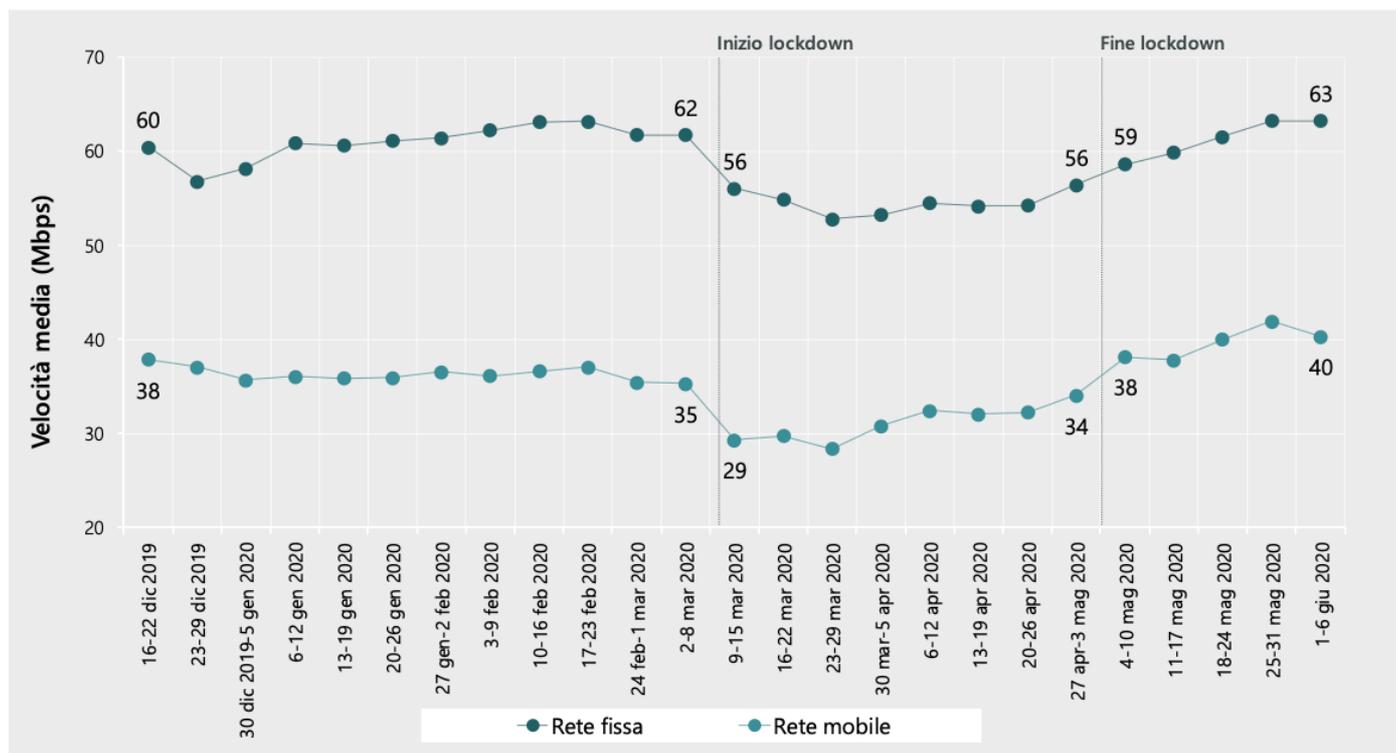


Fonte: AGCOM

<sup>6</sup> Allegato (6 e 7) alla relazione annuale, AGCOM, 2020.

<sup>7</sup> Reti di telecomunicazioni e Covid-19. Così le infrastrutture italiane hanno retto all'onda d'urto del lockdown, 20 novembre 2020, Istituto per la Competitività.

Grafico 4 - Velocità di Download rete fissa e mobile gennaio-giugno 2020.



Fonte: AGCOM

Nonostante sia stato osservato un deterioramento generale delle *performance* delle reti, la continuità del servizio è stata comunque ampiamente garantita, così come testimonia l'analisi effettuata da MedUX<sup>8</sup>. Le stime parlano di un calo della velocità di *download* del 10% (da 61 Mbps a 56 Mbps) nelle ore di punta (20:00-21:00) a livello nazionale (8% per i servizi FTTH), ma anche di un aumento della latenza, ossia dell'intervallo di tempo che intercorre tra quando viene inviato un *input* e quando viene ricevuto il segnale di *output*. Questo aumento, nei giorni di maggiore utilizzo, è stato del 50% nelle ore del mattino e del 150% nelle ore pomeridiane.

Le reti mobili hanno subito un impatto che, sebbene inferiore a quello registrato sulle reti fisse, ha mostrato un aumento del traffico dati oscillante tra il 20% e il 30%, attribuibile principalmente agli utenti *mobile only*. Anche in questo caso si è osservato un calo della velocità di *download* pari all'11,5%, passando da 36,4 Mbps nel periodo *pre-coronavirus* ai 32,2 Mbps durante la fase di *lockdown* [Grafico 4].

Un importante elemento che ha contribuito ad alleggerire la pressione sulla rete è stata la decisione di ridurre la qualità dello *streaming* video, ovvero la riduzione del *bitrate streaming*, presa da alcune piattaforme, come Netflix e YouTube<sup>9</sup>.

<sup>8</sup> TIM, Fastweb, Vodafone, and Wind: Service Degradation in Italy, MedUX, 25 marzo 2020. Report pubblicato su: MedUX.

<sup>9</sup> L'impatto del coronavirus nei settori regolati, AGCOM, 2020.

### 1.3 La società digitale (*gigabit society*) e la banda ultra-larga FTTH

I dati emersi dalle varie analisi evidenziano un buono stato di salute delle infrastrutture mobili italiane, ma è necessario non rallentare lo sforzo in termini di investimenti, soprattutto in ottica 5G.

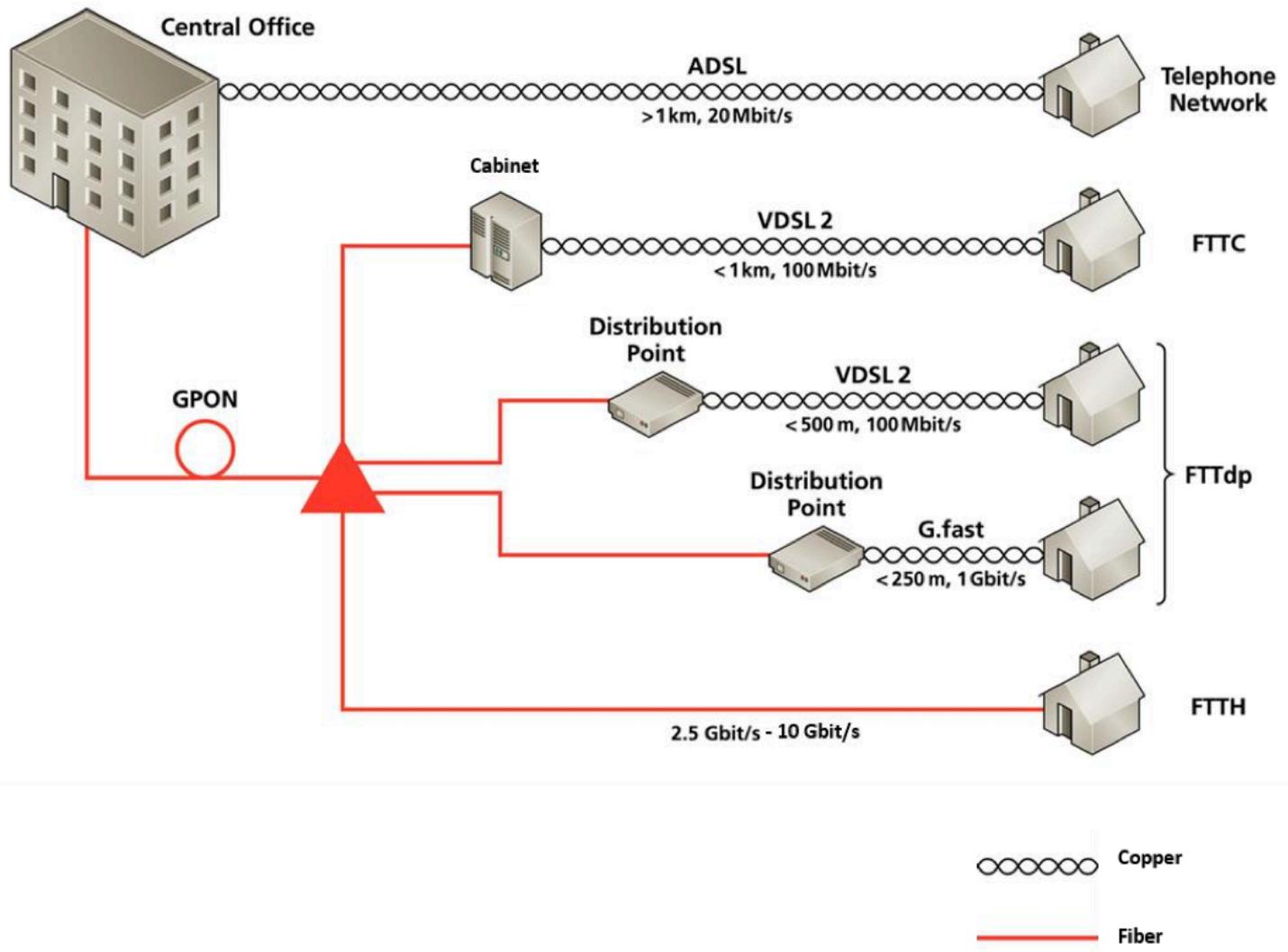
Siamo entrati in una nuova fase dello sviluppo economico e sociale. Ciò è frutto di un continuo e inarrestabile processo di innovazione, che ha caratterizzato nel corso degli ultimi due decenni lo sviluppo di Internet, favorendo la diffusione della *digital economy* in tutti i settori, non più legati soltanto all'ICT. Come avvenuto in passato in ogni rivoluzione tecnologica, il presupposto essenziale è dato dalla disponibilità di infrastrutture adeguate e, nel caso specifico, di un'infrastruttura di telecomunicazioni a banda ultra-larga estremamente affidabile e con una copertura tendente al 100% della popolazione. L'azione sinergica di digitalizzazione e connettività pone il campo delle comunicazioni al centro dei processi di trasformazione. In questo contesto, caratterizzato dall'esplosione della domanda dei servizi video, dalla crescita vertiginosa degli *smart object* dell'*Internet of Things*, dall'introduzione di applicazioni innovative di realtà aumentata (AR) e realtà virtuale (VR), la domanda di dati sta letteralmente esplodendo. L'accesso a Internet tramite un'infrastruttura di telecomunicazioni ad alta capacità, affidabile e capillarmente diffusa rappresenta, dunque, un prerequisito essenziale per essere competitivi, a livello di sistema, nello scenario economico globale.

La crescita vertiginosa del traffico dati, nonché la diversità e molteplicità di esigenze e requisiti dei nuovi attori e servizi della *digital economy*, pongono serie sfide alle reti di telecomunicazioni in termini di banda, latenza, affidabilità e continuità del servizio, in quella che è comunemente definita *Gigabit Society*. Se nei prossimi anni l'Unione Europea vorrà essere *leader*, dovrà sostenere investimenti massicci e su larga scala. La stessa Unione Europea ha fissato precisi obiettivi di connettività entro il 2025 con il fine ultimo di abilitare una serie di nuovi servizi innovativi e pervasivi. Il Boston Consulting Group (BCG) stima che gli investimenti necessari per raggiungere tali obiettivi siano di circa 660 miliardi di euro<sup>10</sup> e la soluzione tecnica individuata per l'accesso fisso a banda larga è *Fiber To The Home* (FTTH) [Figura 5]. In questo senso, grazie alla loro elevata velocità di trasmissione, le infrastrutture in fibra ottica di tipo FTTH agiscono da catalizzatore dei processi di adozione e utilizzo dei servizi digitali per una piena realizzazione della *Digital Economy*.

---

<sup>10</sup> *Building the Gigabit Society: An Inclusive Path Toward Its Realization*, November 2016, Boston Consulting Group (BCG).

Figura 5 - Architetture di rete di accesso fisso.



Fonte: Fraunhofer Institute for Embedded Systems and Communication Technologies ESK, 2014

Solo un'infrastruttura in fibra ottica di tipo FTTH, affidabile e diffusa in modo capillare, può infatti sostenere adeguatamente e con successo tali sfide. Inoltre, la qualità dell'accesso alla rete mobile, in previsione dell'avvento del 5G, difficilmente sarà separata da quello alla rete fissa, conferendo all'infrastruttura in fibra ottica un'importanza fondamentale in termini di "sistema nervoso" delle telecomunicazioni del presente e, soprattutto, del futuro. La fibra ottica fino a casa è l'unica soluzione che permetterà di avere tutta la banda necessaria anche in un futuro non immediato. Si può dire che sia un'infrastruttura definitiva: una volta posata, per aumentarne le prestazioni, basterà soltanto cambiare gli apparati agli estremi<sup>11</sup>.

<sup>11</sup> 5G: no FTTH, no party: ecco perché la fibra fino a casa è l'infrastruttura definitiva, CORCOM, 17 aprile 2018. Articolo pubblicato su: [corrierecomunicazioni.it](http://corrierecomunicazioni.it).

I rilevanti incrementi attesi in termini di intensità d'uso, velocità di trasferimento dati e la drastica riduzione dei tempi di latenza stanno comportando una vera rivoluzione nelle architetture e nelle logiche di gestione delle reti: virtualizzazione delle risorse e densificazione delle stazioni radio base saranno cruciali per i nuovi servizi previsti dallo standard 5G<sup>12</sup>. Senza la fibra che collega le celle che servono gli *smartphone*, infatti, non ci sarebbe il 4G e, soprattutto, non ci potrà essere il 5G, caratterizzato da *performance* di latenza e capacità che, per essere realizzate senza "colli di bottiglia" e sviluppate al massimo delle loro potenzialità, richiederanno reti in fibra ottica capillari per il rilegamento dei siti mobili<sup>13</sup>.

---

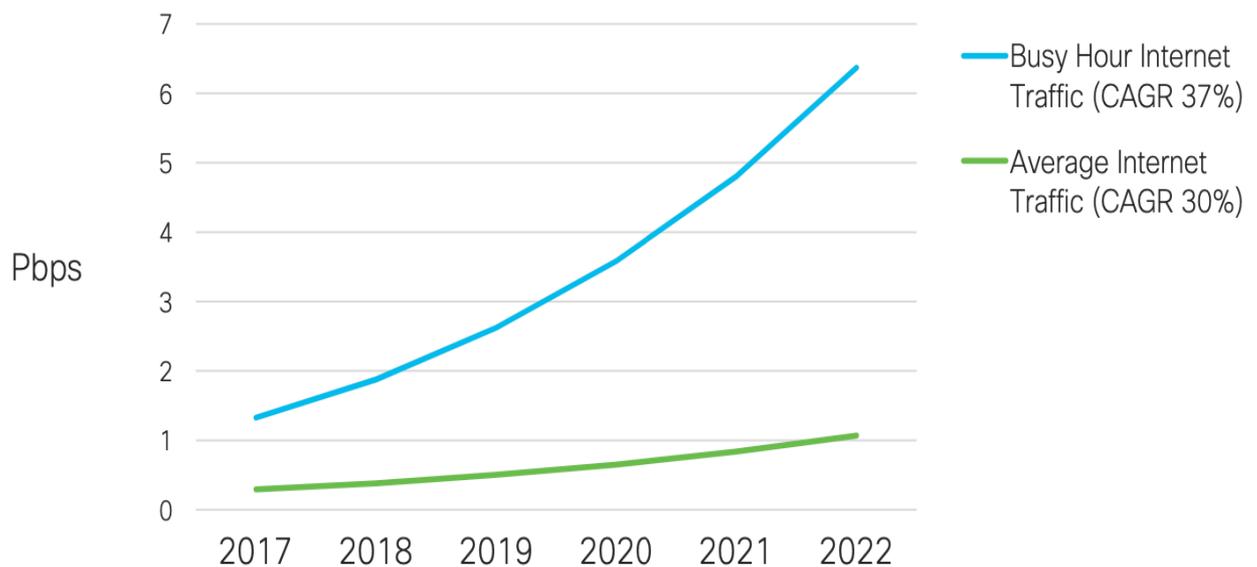
<sup>12</sup> “[T]he faster the DSL technology, the shorter is the distance from the drop point (where the fibre component of the network ends) to the customer that can still be covered on the basis of an upgraded copper network”, Commission Staff Working Document, p. 45.

<sup>13</sup> La Commissione chiarisce che: “la fibra ottica trasmette segnali alla velocità della luce e ha l'efficienza necessaria a garantire connessioni simmetriche e di qualità per decine di chilometri. Le più promettenti tecnologie di miglioramento dei cablaggi in rame hanno attualmente una portata effettiva di circa 250 metri e si basano su fibra nel resto della rete. Le reti ibride fibra-cavo coassiale (HFC), che ricorrono alla serie di standard DOCSIS per migliori prestazioni, si basano su fibra almeno per quanto riguarda il cosiddetto nodale ottico.”

## 1.4 Trend del traffico IP e l'effetto video: panoramica e criticità

Il traffico su rete IP sta facendo registrare un forte aumento e tale *trend* di crescita va ad impattare sulla banda. Negli ultimi 5 anni (2016-2021) si è registrato un aumento del fattore di picco, ossia il rapporto tra la banda di picco e la banda media, del 50% (da 3,9 a 5,53), mentre il traffico medio di Internet è aumentato ma in misura ridotta [Grafico 6].

Grafico 6 - Crescita media del traffico internet e del fattore di picco.



Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

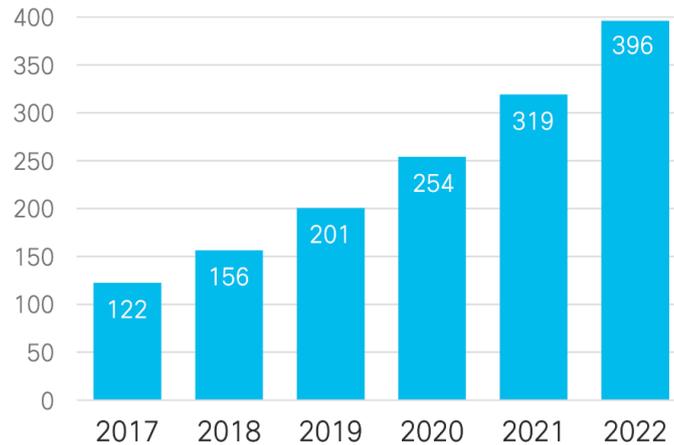
La principale causa di questa grande crescita, amplificata dalla pandemia, è il cosiddetto “effetto video”. Il traffico video in tutte le forme è aumentato drasticamente. Il video funge da motore del cambiamento favorendo la diffusione di reti e servizi sempre più performanti, in grado di soddisfare le crescenti aspettative dei consumatori. Come già osservato all’inizio del decennio 2010 negli Usa e, più di recente (2015) in Europa<sup>14</sup>, si sta assistendo all’esplosione dei servizi video con una crescita consistente in particolare del VoD. Il video *on Demand* (VOD), il *live streaming* (*linear tv*) ed il *gaming* assieme rappresentano circa l’80% del traffico su rete IP. L’effetto dirompente determinato dall’incremento del traffico video sulla rete continua ad essere un tema focale per lo sviluppo non solo del mercato dell’*online entertainment*, ma dell’intero sistema Internet.

<sup>14</sup> *Il VoD in Europa 2015-2018*, Rapporto di ITMedia Consulting.

Grafico 7 - Crescita del traffico IP.

26% CAGR  
2017-2022

Exabytes  
per Month



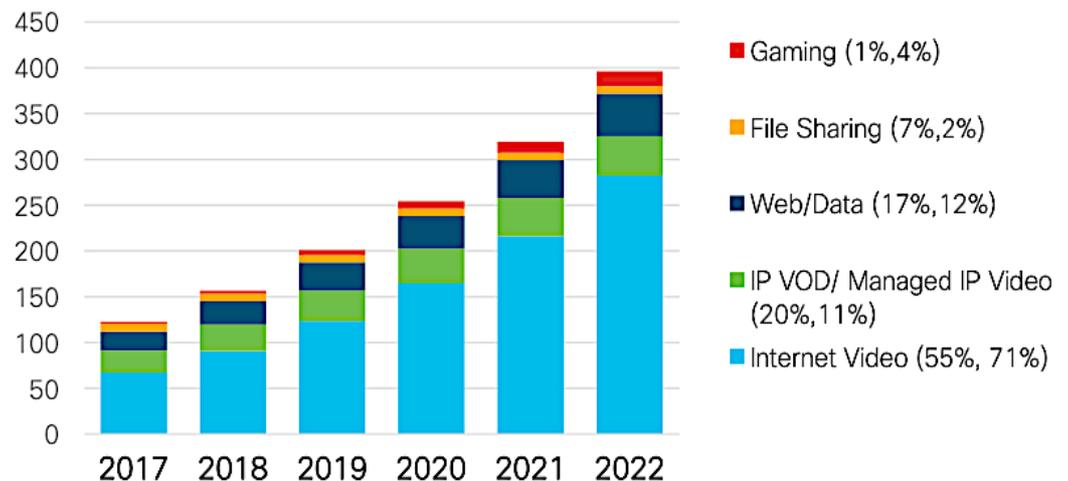
Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

Le previsioni di Cisco riguardo la crescita del traffico IP [Grafico 7] sono state confermate ed i maggiori *driver* di crescita saranno legati al peso dominante dei servizi video e delle connessioni *Machine-to-Machine* (M2M) a supporto delle applicazioni IoT. Più specificatamente, si stima che la somma di tutte le forme di IP video (Internet Video, IP VOD, *file* video scambiati via *file sharing*, servizi di videoconferenza e video *streaming* in ambito *gaming*) conterà tra l'80% e il 90% dell'intero traffico IP arrivando all'82% entro il 2022 [Grafico 8].<sup>15</sup>

Grafico 8 - Trend e forme del traffico IP video.

26% CAGR  
2017-2022

Exabytes  
per Month

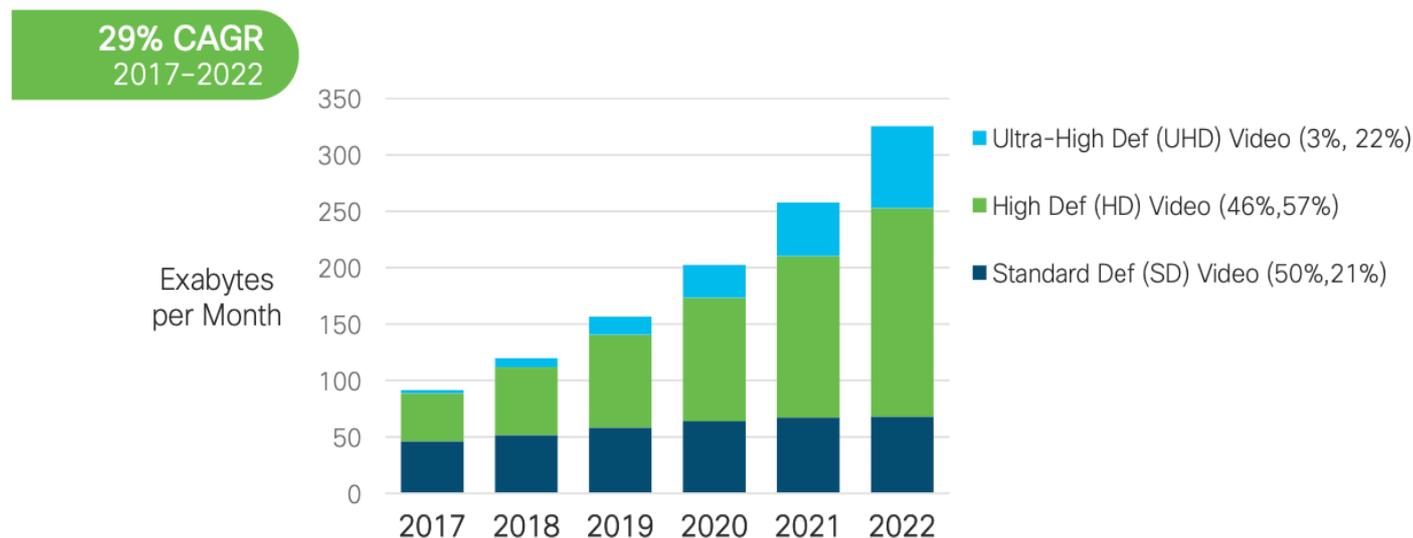


Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

<sup>15</sup> Cisco annual internet report, 2017-2022, Cisco, 2019.

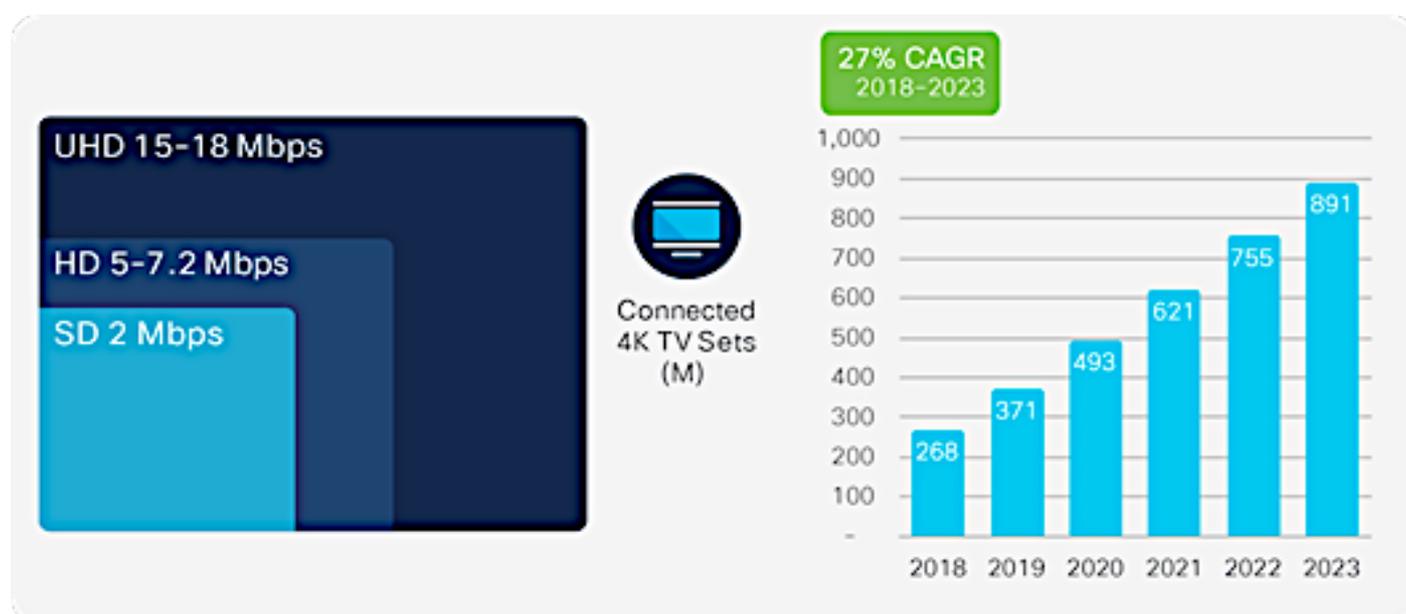
Nel segmento VOD, la spinta alla banda deriva dall'aumento dei video HD (*high definition*) e UHD (*ultra-high definition*, 4K) a scapito della *standard definition* (SD) [Grafico 9]. La tecnologia HD e UHD determina tale effetto perché il *bit rate* per video 4K a circa 15-18 Mbps è più del doppio del *bit rate* video HD e nove volte superiore al *bit rate* video *Standard-Definition* (SD) [Grafico 10]. Si stima che entro il 2022 quasi i due terzi (62%) dei televisori a schermo piatto installati saranno UHD, rispetto al 23% nel 2017 [Grafico 10]. UHD (o 4K) IP VoD rappresenterà il 22% del traffico video IP globale e almeno il 35% del traffico IP VoD entro il 2022.

Grafico 9 - Sviluppo dell'UHD e dell'HD.



Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

Grafico 10 - Servizi video e relativi TH per cliente attivo e numero di tv 4K installate.



Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

Il passaggio a contenuti di elevata qualità ed il progressivo abbandono dei contenuti con SD sta determinando un aumento considerevole del *Throughput* (TH), ossia la capacità di trasmissione effettiva o quantità di dati trasmessi in un'unità di tempo per cliente attivo (Mbps/cliente attivo), che andrò ad analizzare più approfonditamente nel paragrafo successivo. L'aumento di traffico IP globale e l'impatto di tale crescita sulla banda sta generando una duplice criticità:

1. L'aumento del Fattore di Picco, ossia i picchi di traffico che la rete IP fa registrare, fa crescere il costo della rete TCO (*total cost of ownership*). Tali costi dipendono sostanzialmente da:
  - Topologia, tecnologie e architettura, che vanno a stabilire il costo unitario dei segmenti.
  - Banda di picco (Gbps), che a sua volta dipende dal volume di traffico e dalle applicazioni di utente che determinano il fattore di picco.
  
2. La differenza di *bit rate*, che corrisponde alla velocità in Mbps del canale di comunicazione tra una sorgente e una destinazione, tra l'accesso *ultrabroadband* (UBB) rispetto al resto della rete IP, la quale è composta da:
  - Aggregazione = ha lo scopo di effettuare un'aggregazione efficiente del traffico.
  - Metro = il segmento metro/regionale, aggrega il traffico proveniente dalla rete di accesso verso i PoP nei quali sono presenti i nodi di servizio.
  - Core = Rappresenta la dorsale della rete, la rete di lunga distanza (*backbone*) che collega i PoP fra loro e i *gateway* internazionali verso Internet.

Oggi i valori di riferimento del *bit rate* sono:

- Da 20-30 Mbps/utente attivo fino a 150-200 Mbps/utente attivo per reti di accesso UBB fisso e mobile.
- Da 2 Mbps/utente attivo fino a 8-10 Mbps/utente attivo per reti di aggregazione, metro e *core*.

Il fattore di picco (FP) e la differenza di *bit rate* sono critici per:

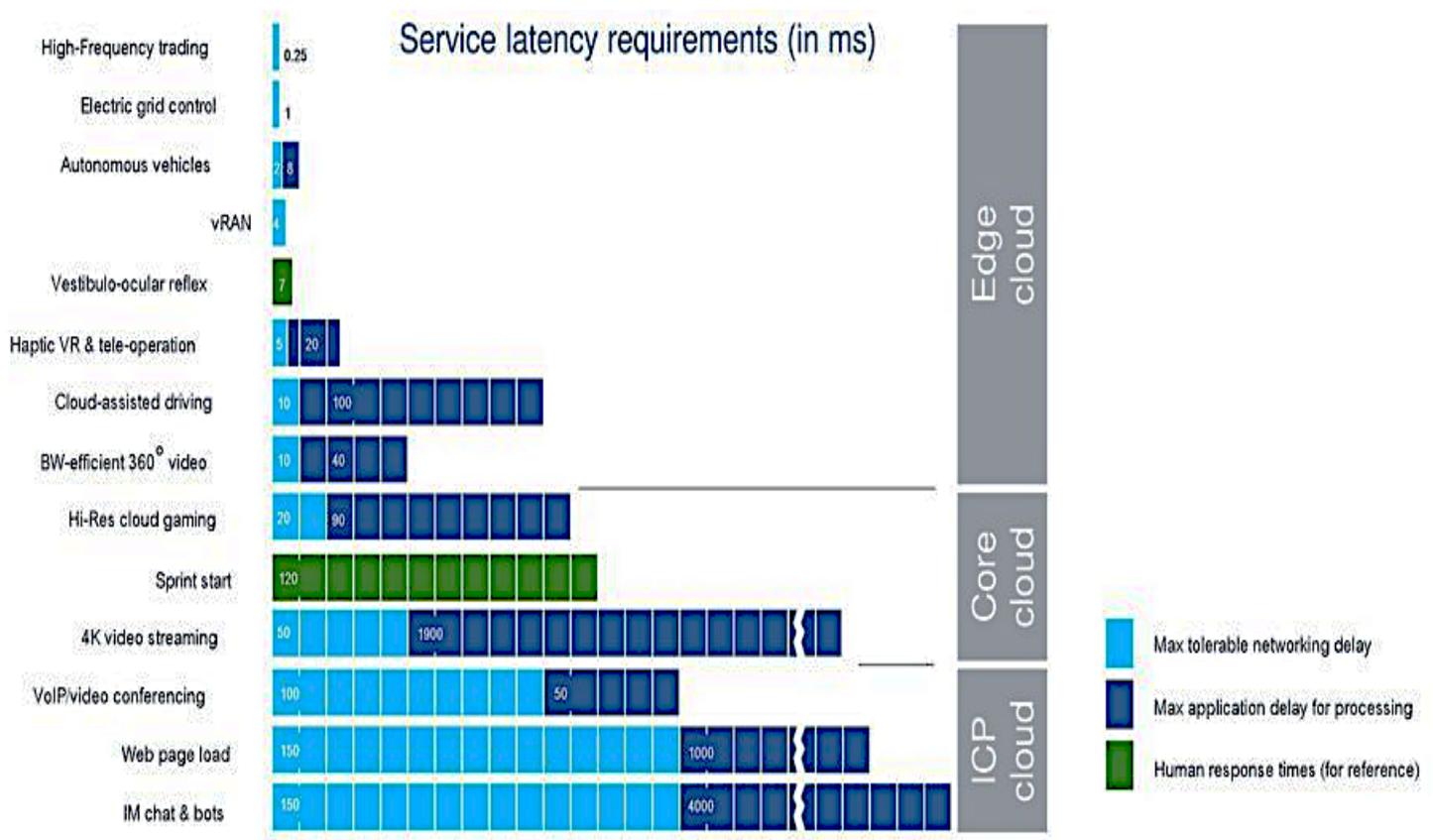
- *Total cost of Ownership* (TCO)
- Prestazione delle applicazioni
- Monetizzazione dell'UBB

## 1.5 La nuova sfida: la *Quality of Experience (QoE)*

Gli sviluppi tecnologici si susseguono ad una velocità frenetica, a partire dall'esplosione della domanda dei servizi video, alla realtà virtuale (VR), fino all'*Internet of Things*. Tradizionalmente il principale *driver* di trasformazione ed evoluzione delle tecnologie ICT è stato essenzialmente di tipo *consumer*, ma l'attuale trasformazione digitale presenta anche una dimensione di tipo industriale, ovvero legata alle esigenze industriali e di produzione, dando luogo a servizi e applicazioni con requisiti estremamente eterogenei.<sup>16</sup>

Ad esempio, nel giro di pochi anni le persone potrebbero partecipare a riunioni d'affari nella loro auto *driverless* esattamente come se fossero in ufficio, grazie alle applicazioni di realtà virtuale. Come affermato precedentemente, siamo all'inizio di una nuova importante fase di sviluppo di Internet, caratterizzata da una pluralità di attori e servizi ciascuno dei quali con specifici requisiti in termini di banda e latenza [Figura 11].

Figura 11 - Requisiti di latenza per servizi e applicazioni.



Fonte: Nokia Bell Labs Consulting, 2016

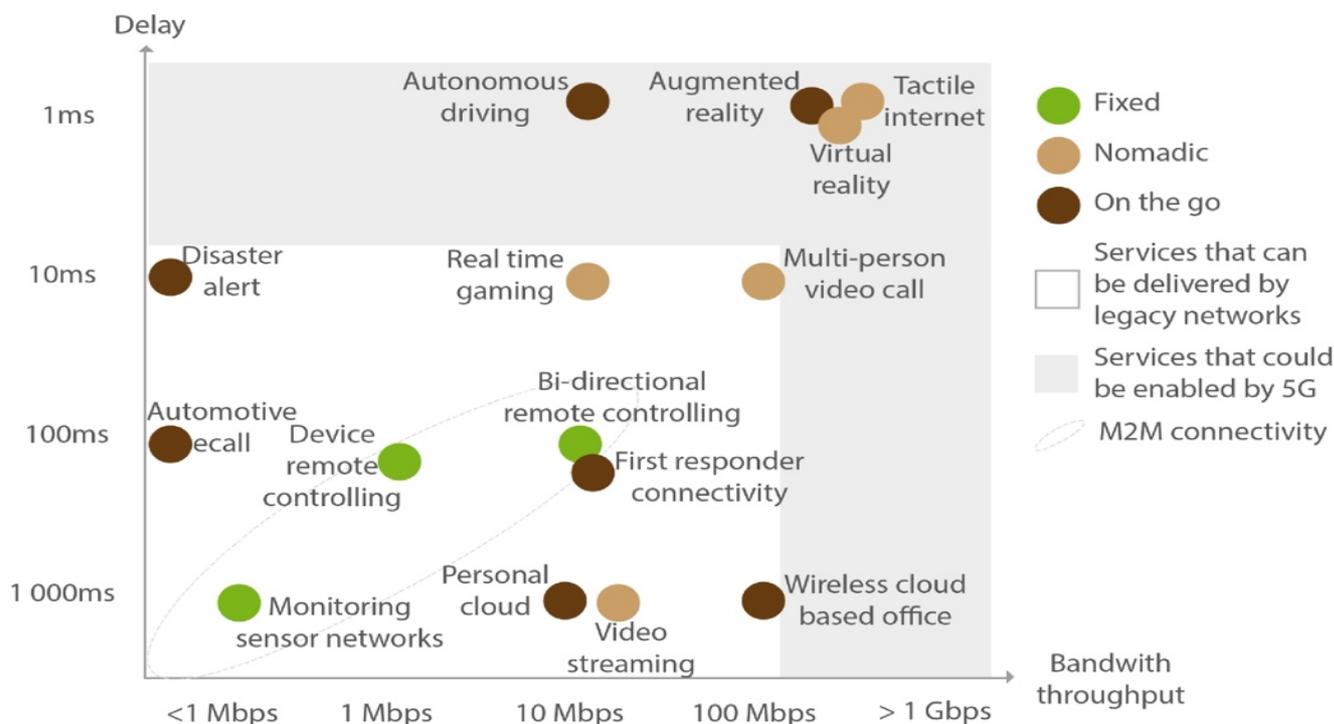
<sup>16</sup> La migliore regolazione per lo sviluppo della gigabit society. Tecnologie abilitanti, evoluzione dei servizi e best option infrastrutturali, marzo 2018, ITmedia consulting e LUISS dream.

Le nuove applicazioni (video ad alta qualità, guida autonoma, realtà aumentata) che si affermeranno con l'avvento del 5G hanno requisiti prestazionali crescenti [Figura 12]. Due sono i principali KPIs<sup>17</sup>:

- Latenza: l'intervallo di tempo che intercorre tra quando viene inviato un *input* e quando viene ricevuto il segnale di *output*, ovvero la velocità di risposta di un sistema a un impulso.
- *Throughput*: la velocità dell'applicazione o del servizio applicativo (misurata in Mbps) ed è riferita ai livelli L4 (trasporto dell'applicativo) e L5 (applicativo) dello *stack* dei protocolli IP. Per le reti di telecomunicazioni, il *Throughput* è riferito in genere al livello 4 (L4) poiché, se il dimensionamento dei *server* che forniscono i servizi applicativi è adeguato, la riduzione di TH dovuta al livello 5 è molto bassa. Il TH dell'applicativo è sempre minore o uguale al *Bit rate* (il *Bit Rate* è il limite fisico del TH) e, nel caso di reti UBB, il TH dell'applicativo è in genere molto minore del BR a causa del controllo di flusso che deve evitare la congestione della rete IP.

Il TH dipende da: *Round trip time* (RTT), *Packet loss* (PL), numero di *Byte* di un pacchetto e il tipo di protocollo usato per il trasporto dell'applicativo (L4). Poiché per uno specifico applicativo sono definiti, dai KPI dell'applicativo, sia il protocollo di L4 che la dimensione dei pacchetti (numero di *Byte*), in genere si dice che il TH dipende da RTT e PL, che andrò ad analizzare nello specifico di seguito.

Figura 12 - Bandwidth and latency requirements for generic applications.



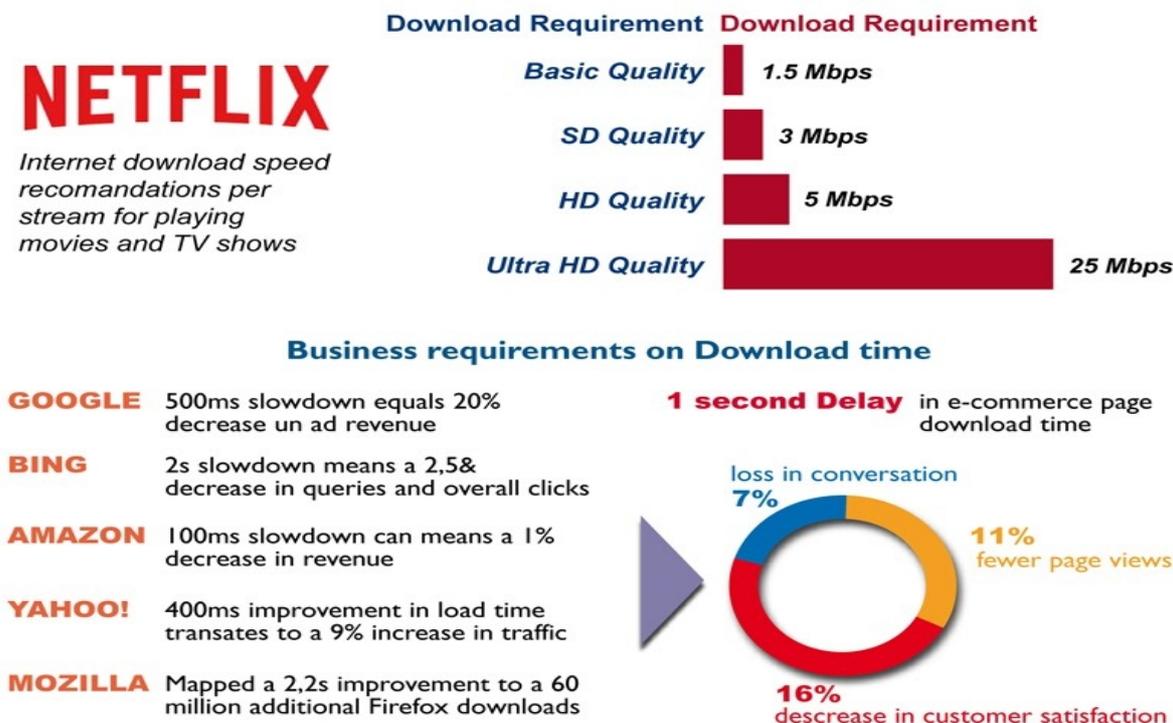
Fonte GSMA Intelligence, 2015, Members' Research Service Page 4 of 9

<sup>17</sup> *Evoluzione della rete ICT*, rivista dell'AEIT, luglio/agosto 2019.

In questo scenario, l'accesso a Internet tramite una rete che sia veloce, affidabile e ad alta capacità è un prerequisito imprescindibile per essere competitivi. Secondo l'ultima versione del Digital Economy and Society Index (DESI)<sup>18</sup>, in Europa la banda larga fissa raggiunge il 98% degli europei e il 76% delle case del vecchio continente ha accesso alla banda ultra-larga (almeno 30 Mbps). Le reti radiomobili 4G coprono in media l'84% della popolazione dell'Unione Europea. Il 74% delle abitazioni in Europa ha un abbonamento alla banda larga fissa e oltre un terzo di queste connessioni è relativo alla banda ultra-larga. Per assicurare la *Quality of Experience* attesa dai consumatori e dall'IoT, sono necessari elevati valori di *throughput* e un *download time* minimo. Gli OTT per lo sviluppo del proprio *business* hanno bisogno che gli *end-user* possano fruire con adeguata QoE i contenuti e le applicazioni che essi offrono.

Avere elevati *throughput* e bassi *download time* è importante non solo per servizi video *streaming*, ma anche per il *web browsing*, poiché alla QoE sono legati incrementi dei ricavi da servizi offerti a *end-user* e *advertising*. Esiste infatti una correlazione tra *Application Throughput* e *download time* e la propensione al consumo e la scelta di consumo dell'*end-user*. Nell'*e-commerce*, ad esempio, un secondo di ritardo nel *download time* determina una riduzione dell'11% per quanto riguarda le pagine visitate ed una riduzione del 16% nella soddisfazione del consumatore [Figura 13].<sup>19</sup> Ritardi come questi possono costituire in determinati casi semplici inconvenienti, ma tradursi in consistenti perdite economiche per i servizi OTT e *web browsing* e generare vere e proprie catastrofi nel caso delle automobili *driverless*.

Figura 13 - Valore commerciale dei parametri di qualità "throughput" e "download time".



<sup>18</sup> Report on European Analysis 2020, Desi (Digital Economy and Society Index) 2020.

<sup>19</sup> Elaborazioni IT Media Consulting su fonti varie, 2014.

## 1.6 Come assicurare una elevata QoE?

L'*application throughput* (TH) è il parametro (KPI) che ha il maggior impatto sulla QoE. Il valore di TH è sempre più basso del *bit rate* (BR), che corrisponde alla velocità in Mbps del canale di comunicazione tra una sorgente e una destinazione, ed in alcuni casi anche molto più basso. Aumentare il BR nelle reti d'accesso è una pre-condizione per il miglioramento delle prestazioni delle applicazioni. Tuttavia, ad elevati valori di BR in accesso devono corrispondere adeguati valori di BR nelle reti di aggregazione, metro e *core* e questo richiede importanti investimenti. Per tale motivo, l'incremento del *Bit rate* nell'accesso e nella rete IP e l'utilizzo di tecniche di *traffic management* (attraverso meccanismi che migliorano la *Quality of Service* (QoS)) non sono sufficienti per migliorare la QoE, ma è necessario agire al di sopra del livello *network* del protocollo OSI (livello 3)<sup>20</sup>.

Per garantire all'*end-user* una QoE elevata è necessario aumentare l'*Application throughput* (TH) attraverso una riduzione dei valori di:

- RTT: nelle reti IP è il tempo (misurato in ms) impiegato da un pacchetto per percorrere il cammino sorgente-destinazione-sorgente. L' RTT dipende essenzialmente da:
  - Distanza tra sorgente e destinazione.
  - Variazioni del cammino seguito dai pacchetti IP per andare dalla sorgente alla destinazione e viceversa.
  - Lunghezza delle code all'interno dei *router*.
- *Packet loss*: indica il numero di pacchetti persi nel cammino sorgente-destinazione-sorgente a causa degli errori di trasmissione e delle code nei *router*. La sua riduzione è molto difficile.

A tal fine è necessario avvicinare i contenuti e le applicazioni ai clienti [Figura 14].

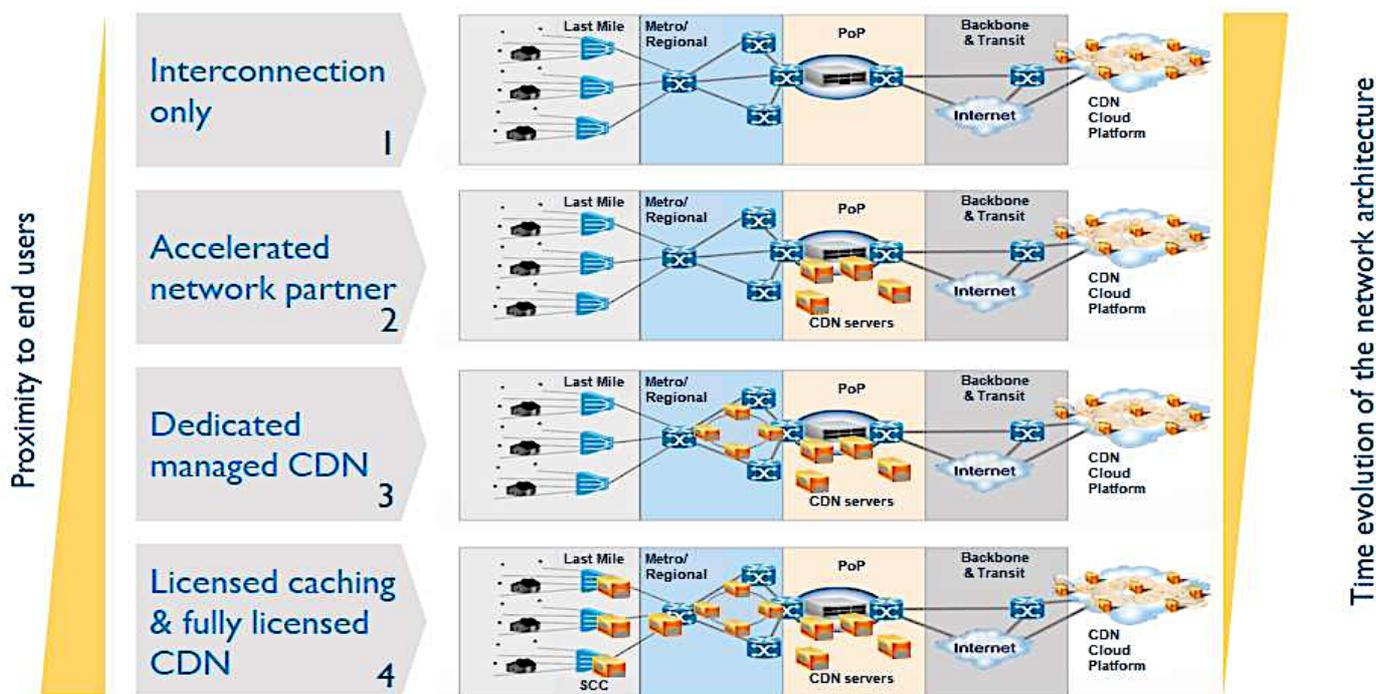
Grazie alle piattaforme di CD, distribuite in modo capillare nella rete (*deep into the network*), si riesce ad ottenere un valore più basso di RTT e di *packet loss*. Riducendo la distanza fra il contenuto e l'*End-user* si migliora la QoE e, in molti casi, si riducono i costi. Inoltre, attraverso l'utilizzo di piattaforme di *transparent caching*, si riduce la banda di picco sulla rete del Telco e questo diminuisce i costi della rete.

Per chiarire come funziona il *transparent caching*, possiamo prendere ad esempio le pagine Html che possono richiamare un numero molto elevato di oggetti (testi, figure, filmati), eventualmente provenienti da più *server web*. Di questi oggetti, un certo numero può rimanere invariato nel tempo ed essere riutilizzato in più pagine (si pensi ad esempio a contenuti statici come i loghi). Per rendere più veloce il caricamento delle pagine ed occupare meno risorse della rete di trasporto IP, si può mantenere in una memoria locale questi oggetti statici e riutilizzarli all'occorrenza: è quanto fa normalmente il *browser*, che conserva gli oggetti in una *cache* del PC.

---

<sup>20</sup> Verso la rete dei contenuti, notiziario tecnico, Gruppo Tim.

Figura 14 - Evoluzione dell'architettura della rete.



Fonte: Akamai

Portando il contenuto o le applicazioni vicino agli *end-user* si riduce la latenza, determinando un miglioramento nelle *performance* in termini di TH, RTT, *Download Time*.

Di fronte alla necessità di migliorare la QoE, vi sono due principali approcci:

1. Approccio tradizionale dei Telco: obiettivo principale è quello di incrementare il *bit rate* e le funzionalità dei QoS. Si riscontra però in tale approccio un miglioramento della *performance* ridotto e un elevato Total Cost of Ownership (TCO) e Time To Market (TTM). Infatti, il miglioramento del TH è basso, il rapporto TH/*BitRate* diminuisce e il rapporto Costo/*BitRate* aumenta.
2. Approccio *Edge Computing*: attraverso la distribuzione di IP *Edge functionalities* e *Content Delivery platform* si registra un miglioramento delle *performance* con un TCO ed un TTM contenuti. In questo caso il rapporto TH/*BitRate* aumenta mentre il rapporto tra costo/*BitRate* diminuisce.

L'*IP edge computing* consente l'utilizzo di piattaforme di CD che possono determinare un importante aumento del TH e, nella maggior parte dei casi, un risparmio sui costi. Per questo l'obiettivo degli OTT e dei CDN *Provider* è di inserire le proprie piattaforme per la QoE (*server/cache/acceleratori*) a partire dai *Data center*, per poi entrare nei POP (*Point-of-Presence*), ossia i punti di interconnessione fra i vari segmenti della rete Telco, ed avvicinarsi il più possibile agli *end-users*. Questo bisogno di migliorare la QoE è una importante opportunità per i Telco che possono offrire agli OTT servizi di *delivery* con qualità differenziata. Per cogliere questa opportunità i Telco devono da un lato dotarsi di soluzioni idonee per assicurare *delivery* ad alta qualità (piattaforme per la QoE), dall'altro adottare nuovi modelli di interconnessione IP.

I modelli di interconnessione IP tradizionali tra Telco e OTT sono basati su accordi di transito e *peering, free* oppure *paid*, e sulla terminazione del traffico in modalità “*best effort*” (i pacchetti vengono consegnati a destinazione “al meglio”, compatibilmente con le condizioni del traffico e della rete: non vi sono garanzie che i pacchetti siano trasportati con predefiniti livelli di qualità). Tale tipologia di interconnessione era adeguata quando lo scenario delle telecomunicazioni era ancora prevalentemente “*voice centric*”. Il passaggio ad uno scenario “*data centric*” ha modificato radicalmente le regole del gioco. Questa trasformazione ha visto la comparsa e l'affermazione di aziende OTT/CP (*OverTheTop e Content Providers*) che forniscono servizi, applicazioni, contenuti in Internet e possono raggiungere ed essere raggiunti dai clienti finali grazie alla connettività mondiale garantita dalle reti interconnesse degli Operatori nazionali ed internazionali. Nell'ecosistema degli OTT/CP si verifica una progressiva concentrazione attorno ad alcuni grandi *player* (i cosiddetti *Hypergiants*), con la conseguenza che la gran parte del traffico IP sulle reti dei Telco nazionali proviene dall'esterno delle reti stesse (cioè dai *server* degli *Hypergiants*).

In questo contesto l'utilizzo dei modelli tradizionali di interconnessione mostra limiti crescenti e determina situazioni di criticità, in particolare per due aspetti.

1. La sostenibilità economica delle Telco.

I Telco sembrano essere in sofferenza. Fanno registrare utili inferiori agli OTT, sostengono investimenti molto più elevati degli OTT e la loro capitalizzazione è inferiore agli OTT. Riescono a mantenere i ricavi rinunciando talvolta agli utili e ricorrendo sempre più all'indebitamento come leva finanziaria. Ciononostante, restano i detentori dell'infrastruttura (oltre che, di fatto, della gestione del cliente finale) che consente all'intero mercato, OTT compresi, di funzionare. Senza i loro investimenti in tecnologia evolutiva e manutentiva l'intero mercato non avrebbe possibilità di sostenersi e svilupparsi (si pensi alle reti di nuova generazione in fibra ottica e alla enorme quantità di investimenti che richiederanno). Il traffico generato da OTT/CP attraversa interconnessioni di tipo *transit* (pagate dalle Telco) o di tipo *peering* in generale non remunerate; solo in qualche caso le Telco ricevono cifre modeste (*paid peering*) per il servizio di *delivery* del traffico sino ai clienti finali. L'inadeguatezza dei modelli di interconnessione tradizionali è testimoniata anche da diversi contenziosi (fra Telco e OTT, aggregatori/CDN *Providers* internazionali), che vengono risolti introducendo nuovi modelli di interconnessione, talvolta solo dopo l'intervento delle Autorità.

2. I livelli di qualità con cui gli *end-user* riescono a fruire di applicazioni, servizi, contenuti “IP-based”.

I modelli di interconnessione tradizionali sono basati sulla terminazione IP di tipo “*best effort*”. Questa modalità è sufficiente per alcune tipologie di traffico, ma può risultare inadeguata per applicazioni/contenuti che hanno elevati requisiti di qualità di fruizione, come ad esempio servizi video ad alta definizione, servizi ad alta interattività, *gaming*, *cloud* pervasivo, navigazione *web* con stringenti requisiti di *download time*.

È significativo rilevare che proprio l'inadeguatezza dei modelli di interconnessione tradizionali ha favorito l'affermazione di soggetti (es. Akamai, Limelight, CloudFlare) che offrono, a livello globale, servizi di *delivery* di traffico IP assicurando una qualità migliore di quella ottenibile con un trasporto *end-2-end* di tipo "best effort", ad esempio mediante soluzioni di *cacheing*, *web acceleration*, *Content Delivery Network*.

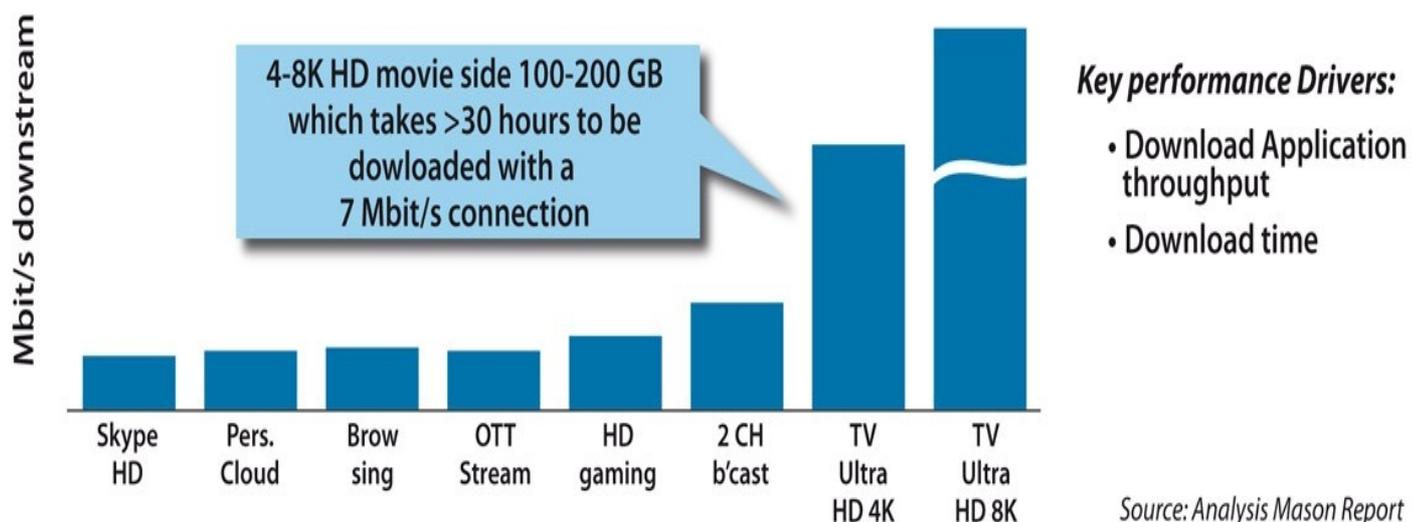
Queste soluzioni sono utilizzate non solo per servizi "bandwidth intensive" come il video *streaming*, ma anche per migliorare la fruibilità di servizi Internet tradizionali come il *web browsing*.

Il "tempo di risposta al *click*", come già in precedenza analizzato, è un parametro fondamentale per qualunque *business* legato alla navigazione Internet e per qualunque OTT/CP che voglia aumentare il proprio *footprint*, in termini di numero, durata, soddisfazione delle frequentazioni dei propri siti da parte dei clienti finali.

Per favorire la soluzione delle criticità relative alla sostenibilità economica delle Telco e per assicurare che i clienti finali possano accedere con un'adeguata QoE ai contenuti ed alle applicazioni su Internet, sono necessari nuovi modelli di interconnessione, capaci di abilitare nuovi modelli di *business* e di valorizzare gli *asset* sia degli operatori di telecomunicazioni (clienti finali ed infrastruttura di rete), sia degli *Over-The-Top* (contenuti, applicazioni, *global reach*). Nei nuovi modelli, accanto alla tradizionale terminazione "best effort", *free-peering*, *paid-peering* e transito, sono disponibili servizi di terminazione IP con qualità differenziata e nuovi modelli di *business* (*revenue sharing*, *content delivery services*), adeguati ai livelli di QoE e ai requisiti prestazionali delle nuove applicazioni/servizi, relativi in particolare a [Figura 15]<sup>21</sup>:

- l'effettiva velocità con cui un utente utilizza un applicativo (cioè il *throughput* a livello applicativo);
- il tempo di scaricamento delle pagine *web*, filmati, contenuti, ecc... (cioè il *download time*).

Figura 15 - Esempio di requisiti di throughput.



Fonte: Analysis Mason Report

<sup>21</sup> Nuovi modelli di interconnessione IP, notiziario tecnico, Gruppo Tim.

I nuovi modelli di interconnessione consentono alle Telco/ISP di avere ricavi sia da *end-user* sia da OTT/CP, in relazione agli specifici benefici che i diversi soggetti ottengono. Le modalità di terminazione offerte da Telco/ISP possono essere utilizzate da qualunque OTT/CP in linea con i principi della *Net Neutrality*. Esempi di nuove modalità di interconnessione fra Telco/ISP ed OTT/CP sono: interconnessione Netflix con Comcast, Verizon ed altri Operatori; interconnessione Cogent/Orange; interconnessione Google/Orange; interconnessione di Akamai con Verizon, ATT, Orange ed altri Operatori; l'attività di *depeering* realizzata praticamente da tutte le Telco/ISP.

Il passaggio ai nuovi modelli è spesso accompagnato da contenziosi legali tra Telco/ISP e OTT, che hanno generato dibattiti, ancora in corso, sulla *Net Neutrality*.

Su questo importante tema, in Europa e negli USA lo scenario si presenta diverso. In Europa il dibattito sugli obblighi che la *Net Neutrality* pone alle Telco (non agli OTT) è tra:

- *Soft Net Neutrality* definita come “la capacità per un *consumer* di avere accesso e distribuire informazioni o eseguire applicazioni e servizi a sua scelta”<sup>22</sup>.
- *Strong Net Neutrality* vista come un insieme di restrizioni/obblighi al trattamento del traffico Internet: “tutto il traffico Internet è trattato allo stesso modo, senza discriminazioni, restrizioni o interferenze, indipendentemente dal suo mittente, destinatario, tipo, contenuto, dispositivo, servizio o applicazione”<sup>23</sup>.

In USA l'orientamento appare verso la *Soft Net Neutrality*. Se il dibattito in Europa finisse per far prevalere un'interpretazione *strong* della *Net Neutrality* e se essa fosse riferita anche ai livelli superiori al livello “Network” (Livello 3), ci sarebbe il rischio di restrizioni per le Telco sull'utilizzo di piattaforme per QoE. Le reti domestiche delle Telco non potrebbero così soddisfare i “*services requirements*” di alcune applicazioni o contenuti e sarebbero penalizzate rispetto agli OTT.

I nuovi servizi potrebbero essere forniti solo se le piattaforme per QoE degli OTT fossero realizzate dagli OTT stessi ed inserite nelle reti dei Telco vicino agli *end-user*. Questa lettura restrittiva della *Net Neutrality* impedirebbe alle Telco di monetizzare la terminazione con qualità differenziata (QoE) sia lato OTT, sia lato *end-user*. Le Telco potrebbero offrire solo il trasporto IP di tipo *best effort*.

Se invece le piattaforme per QoE fossero realizzate dalle Telco, esse sarebbero disponibili per tutte le Telco/ISP, oltre che per OTT/CP, sulla base di accordi commerciali non discriminatori. Si realizzerebbe quindi una vera *Net Neutrality* e un ‘*true level playing field*’.<sup>24</sup>

---

<sup>22</sup> Digital Agenda for Europe website. Fonte: <https://ec.europa.eu/digital-agenda/about-open-internet>.

<sup>23</sup> Regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio del 25 novembre 2015.

<sup>24</sup> *Verso la rete dei contenuti*, notiziario tecnico, Gruppo Tim.

## 1.7 Edge computing

### Cos'è l'*edge computing*?

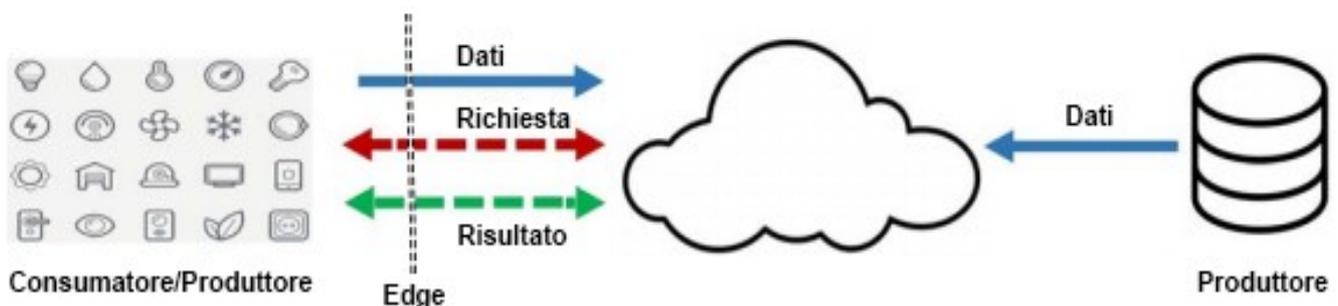
L'*edge computing* è un'architettura IT distribuita con potenza di elaborazione decentralizzata, predisposta per le tecnologie di *mobile computing* e *Internet of Things (IoT)*. Nell'*edge computing* i dati sono elaborati dal dispositivo stesso o da un computer o da un *server* locale e non sono trasmessi al *data center*<sup>25</sup>. L'*edge computing* permette di accelerare i flussi di dati che vengono elaborati in tempo reale con latenza molto bassa o tendenzialmente nulla e consente alle applicazioni e ai dispositivi intelligenti di rispondere quasi istantaneamente, durante la fase di creazione dei dati, eliminando i ritardi: questi elementi risultano fondamentali per tecnologie quali le automobili a guida autonoma. L'*edge computing* consente l'elaborazione efficiente dei dati in grandi volumi in prossimità dell'origine. Ciò determina una riduzione nell'utilizzo della larghezza di banda Internet, l'eliminazione di parte dei costi e la garanzia di un uso efficace delle applicazioni in posizioni remote.

Inoltre, la possibilità di elaborare i dati senza mai trasferirli nel *cloud* pubblico aggiunge un livello di sicurezza utile in particolare per quelli sensibili. La figura 16 illustra gli *stream* di elaborazione in entrambi i sensi tipici del paradigma dell'*edge computing*. In quest'ultimo, le *things* non sono solo consumatori, ma anche produttori.

Nell'*edge* le *things* non possono solamente richiedere servizi e contenuti dal *cloud*, ma hanno anche il compito di eseguire dei *task* per conto di esso. L'*edge* può eseguire *computing offloading*, *data storage*, *caching and processing*, ma anche soddisfare le richieste di consegnare determinati servizi dal *cloud* all'utente.

È chiaro che l'*edge* stesso, quindi, necessita di essere ben progettato per rispettare in modo efficiente i requisiti di servizi quali affidabilità, sicurezza e protezione della *privacy*.

Figura 16 - Flussi di elaborazione tipici del paradigma dell'*edge computing*.



<sup>25</sup>Edge computing: cos'è, come implementarlo e quali vantaggi per le imprese, 18 novembre 2019.

Con l'*edge computing* si vuole, come detto, spostare l'elaborazione dei dati vicino alla loro sorgente. Questo ha diversi benefici se comparato al tradizionale paradigma di *cloud-based computing*. Qui di seguito sono esposti diversi risultati che dimostrano i potenziali benefici del nuovo paradigma<sup>26</sup>:

- Per quanto riguarda le applicazioni di riconoscimento facciale i tempi di risposta sono scesi da 900 a 169 ms, spostando l'elaborazione dal *cloud* verso l'*edge*.
- Per l'assistenza cognitiva indossabile i risultati mostrano che il miglioramento dei tempi di risposta è compreso tra 80 e 200 ms.
- Il consumo di energia potrebbe essere ridotto dal 14% al 25%<sup>27</sup>.

### **Perché l'*edge computing*?**

Collocare tutti i *task* sul *cloud* è provato essere un modo efficiente di processare i dati, considerato che la sua potenza di calcolo surclassa le capacità di ciò che si trova all'*edge* della rete. Tuttavia, se comparata alla velocità di elaborazione dei dati, che è in rapido sviluppo, la larghezza di banda è in pratica in una situazione di stallo.

Con la crescente quantità di dati generati all'*edge*, la velocità nel trasporto dei dati sta diventando il collo di bottiglia per il paradigma di calcolo *cloud-based*. Per esempio, alcuni aerei di linea possono generare circa 5 GB/sec di dati, ma la larghezza di banda tra loro e il satellite o una stazione base che si trova sul suolo terrestre non è sufficientemente elevata per la trasmissione dei dati. Nel caso invece di un veicolo autonomo, come un'auto, esso genera 1 GB/sec di dati e richiede un'elaborazione di essi in tempo reale affinché il veicolo assuma delle decisioni corrette. Se tutti i dati necessitassero di essere inviati sul *cloud* per essere processati, i tempi di risposta sarebbero troppo elevati, senza contare che l'attuale larghezza di banda della rete, nonché la sua affidabilità, verrebbero messe alla prova perché sarebbe necessario supportare potenzialmente molti veicoli all'interno della stessa area. È chiaro che i dati, in questo caso, hanno bisogno di essere processati all'*edge* della rete, in modo tale da avere tempi di risposta più brevi, una più efficiente elaborazione di essi e una minore pressione sulla rete.

Oggi i dispositivi connessi sono 35 miliardi e si stima che fra quattro anni saranno 83 miliardi, pari a una crescita del 130%<sup>28</sup>. Risulta quindi chiaro che la quantità di dati prodotta da essi crescerà esponenzialmente, e il classico modello di *cloud computing* non sarà più in grado di gestirli in modo efficiente.

---

<sup>26</sup> Bellino Massimiliano, *L'edge computing in ambiente IoT, tutti i vantaggi*, 10 giugno 2020.

Articolo pubblicato su: NetworkDigital360.

<sup>27</sup> Torchiani Gianluigi, *L'Edge Computing abilita sostenibilità ed efficienza energetica*, 8 aprile 2021.

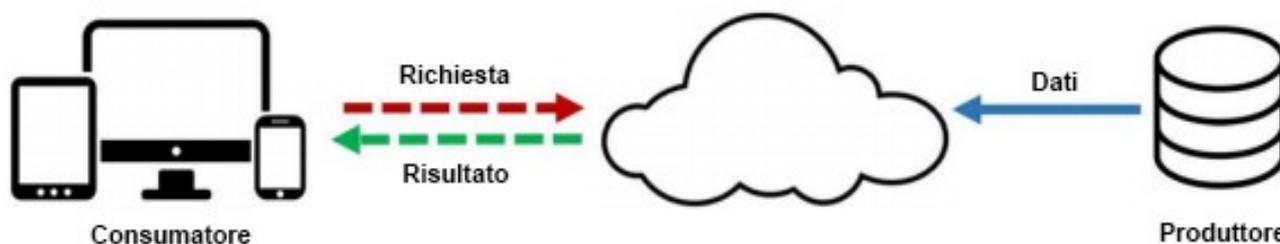
Articolo pubblicato su: NetworkDigital360.

<sup>28</sup> *The Internet of Things: Consumer, Industrial & Public Services 2020-2024*, aprile 2020, Juniper Research.

Ciò significa che gran parte dei dati prodotti nel contesto *IoT* non sarà più trasmessa verso il *cloud*, ma verrà invece consumata nell'*edge* della rete stessa. La figura 17 mostra la struttura del classico *cloud computing*. I produttori generano dati e li trasmettono verso il *cloud*, mentre i consumatori inviano al *cloud* richieste per consumarli.

Le due linee tratteggiate rossa e verde indicano rispettivamente una richiesta di consumo di dati e il risultato che il *cloud* invia al consumatore che ne aveva fatto richiesta in precedenza.

Figura 17 - La struttura del classico *cloud computing*.



Questa struttura non si dimostra sufficiente in ambito *IoT*. Infatti, sono presenti importanti vincoli per il paradigma di *cloud computing*:

- La quantità di dati che si muoverebbe verso il *cloud* è troppo elevata, il che porterebbe a un enorme e non necessaria larghezza di banda nonché ad un uso spropositato delle risorse di calcolo.
- I requisiti in termini di protezione della *privacy* sarebbero un grosso ostacolo all'uso del *cloud computing*.
- I nodi in ambito *IoT* e il modulo di comunicazione *wireless* presentano un elevato livello di consumo energetico, quindi l'*offloading* di parte dei *task* sull'*edge* potrebbe essere molto più efficiente.

Anche il cambiamento del ruolo da solo consumatore a consumatore/produttore sta creando delle necessità che spingono verso l'*edge computing*. Nel paradigma di *cloud computing* i dispositivi finali all'*edge* tipicamente giocano il ruolo di consumatori di dati, basti pensare a quando uno *smartphone* viene usato per guardare un video su YouTube. Oggi, però, le persone oltre a consumare dati con i dispositivi mobili, ne producono. Per esempio è normale che gli utenti scattino foto o registrino video con lo *smartphone* e poi li condividano attraverso servizi basati sul *cloud* come Instagram, YouTube etc. Ogni minuto gli utenti di questi servizi condividono una quantità di foto e video inimmaginabile fino a qualche anno fa. Con lo sviluppo della qualità, ogni foto/video occupa molto spazio in termini di memoria e necessita di una grossa quantità di banda per farne l'*upload*. In questi casi, il *file* dovrebbe essere adattato in termini di risoluzione prima di essere caricato sul *cloud*.

Un ulteriore esempio potrebbe essere quello relativo ai dispositivi medici indossabili. Poiché i dati raccolti da tali dispositivi all'*edge* della rete sono tipicamente privati, processarli nell'*edge* stesso potrebbe aiutare a proteggere meglio la *privacy* dell'utente rispetto a una soluzione in cui essi vengano caricati sul *cloud*.

### ***Edge computing e 5G***

In questo scenario, al 5G è stato da sempre assegnato un ruolo importante quale forma di connettività ad alte prestazioni e, in prospettiva, largamente diffusa. Attualmente diversi analisti sottolineano che proprio la combinazione tra 5G ed *edge computing* potrebbe superare il circolo vizioso che sta frenando lo sviluppo delle reti mobili di nuova generazione<sup>29</sup>. Questa combinazione sdoganerebbe il modello del cosiddetto *Multi-access Edge Computing*, o MEC<sup>30</sup>. Il *Multi-access Edge Computing* è, in estrema sintesi, l'insieme delle applicazioni di *edge computing* basate in larga prevalenza su connettività mobile e non sulle reti fisse. Si punterebbe ovviamente sulla parte radio del 5G come tecnologia che semplifica la connessione dei nodi periferici, perché in questa modalità non è richiesta la presenza diffusa di reti cablate ad alte prestazioni.

La differenza, però, non sta solo nel tipo di connessioni che vengono usate. In prospettiva, possiamo immaginare che ogni singolo *device* di *edge computing* sia dotato di connettività mobile 5G oppure lo sia qualche forma di nodo di rete immediatamente vicino ai *device* stessi.

Il traffico dei dati e delle elaborazioni corrispondenti può essere gestito da un operatore 5G in maniera che resti il più possibile alla periferia della rete, circolando solo tra i siti *edge* e i nodi della rete 5G.

In alcuni casi, potrebbe essere l'operatore 5G stesso a delocalizzare le capacità di *computing* e di *storage* nei suoi nodi *edge*, offrendole alle *software house* oppure ai *content provider* che vogliono portare applicazioni e servizi in periferia.

Secondo Juniper Research<sup>31</sup>, proprio gli operatori mobili investiranno cifre importanti, la stima è di 8,3 miliardi di dollari nel 2025, per lo sviluppo del *Multi-access Edge Computing*.

Oggi, come accennato precedentemente, il problema del 5G è la presenza di un circolo vizioso che non si riesce a sbloccare. Nelle nazioni dove ci sono le reti mancano ancora servizi appetibili in grado di stimolare la domanda. La mancanza di una domanda non stimola chi dovrebbe sviluppare nuovi servizi a portarli sul mercato, così l'offerta del 5G si limita alla disponibilità di una maggiore banda *wireless*, che spinge pochi a mettere mano al portafogli<sup>32</sup>.

---

<sup>29</sup> *Multi-access Edge Computing: la spinta giusta per il 5G?*, 22 gennaio 2021. Articolo pubblicato su: ImpresaCity.

<sup>30</sup> Per alcuni MEC è genericamente *Mobile Edge Computing*.

<sup>31</sup> *Edge Computing: 5G's secret weapon*, white paper, Juniper Research.

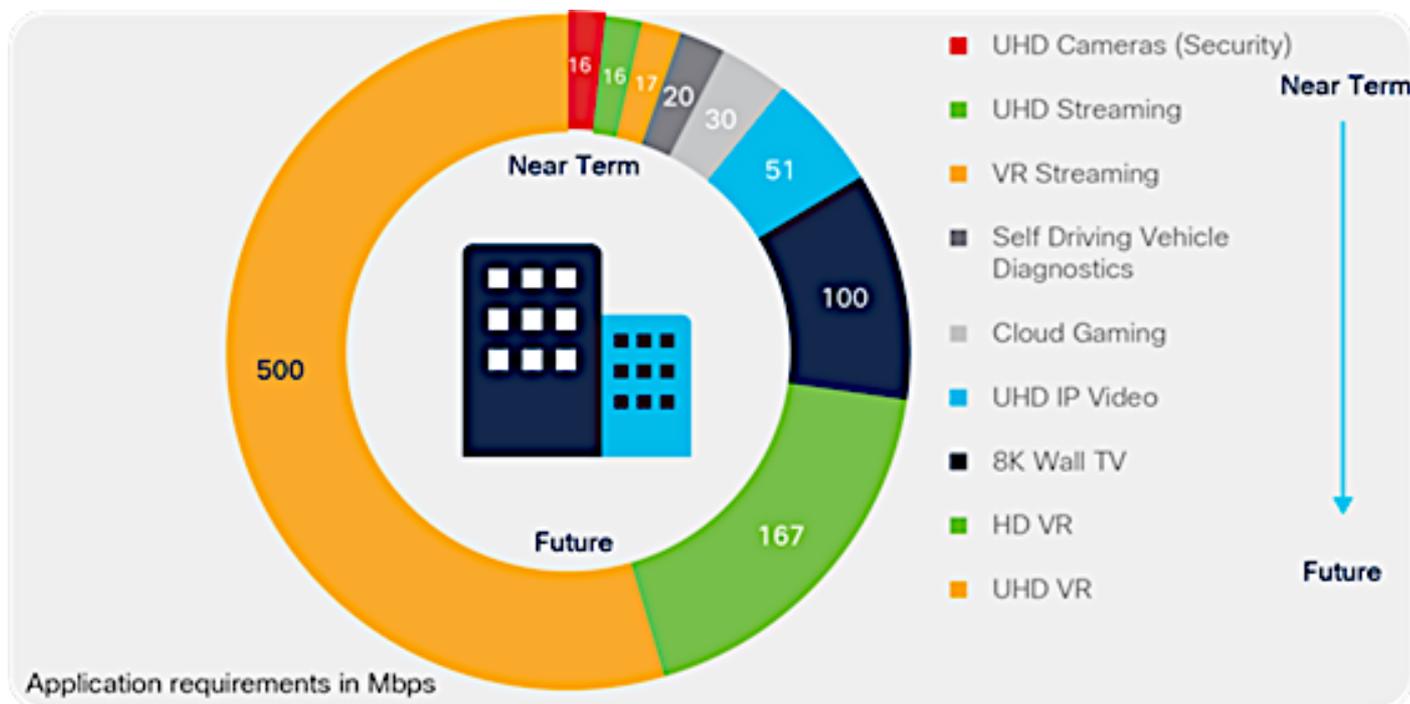
<sup>32</sup> *Reti e servizi 5G: accelerazione o frenata?*, 3 aprile 2020, Articolo pubblicato su: ImpresaCity.

## 1.8 Previsioni

La direzione è ormai tracciata e nei prossimi anni si richiederanno in misura crescente infrastrutture di rete sempre largamente disponibili, più capaci e performanti, in grado di veicolare con elevata affidabilità enormi quantità di contenuti.

Parallelamente si sta assistendo al graduale e inarrestabile passaggio di tutta la produzione a utilità ripetuta (film e serie Tv) dal *broadcasting* al *broadband*, sollevando numerose questioni legate alla gestione del traffico e alla qualità dei servizi (*Net Neutrality*). Secondo i dati di Cisco Systems, gli utenti di video *online*, escludendo quelli di tipo *mobile only*, arriveranno a quota 2 miliardi entro il 2022, a fronte degli 1,4 miliardi del 2016, per una fruizione totale di 3 trilioni di minuti di video al mese. Questa imponente base di utenti necessita e necessiterà di reti ad elevata velocità ed alta affidabilità per sostenere i requisiti sempre più elevati dei servizi video [Figura 18].

Figura 18 - Scenario futuro dei servizi video di tipo home e i relativi requisiti in termini di banda.



Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

Dal punto di vista del mercato in ambito *entertainment*, il successo di Netflix negli Stati Uniti, che occupa oltre 1/3 del traffico nelle ore di punta nel Nord America, e il suo consolidamento nei mercati a livello internazionale ha scosso e messo in discussione le posizioni di forza di numerosi operatori, mostrando le rigidità di un sistema televisivo (*free e pay*) incentrato sul modello *broadcast*.

Operatori televisivi, Telco e produttori di contenuti si stanno attivando secondo strategie di *business* che vedono Internet come una piattaforma alternativa o supplementare ai propri modelli di *business*, ma senza ancora riuscire a coglierne appieno le potenzialità evolutive e di cambiamento.

Sempre Cisco ha aggiornato il suo previsionale annuale sull'evoluzione del mercato della connettività Internet, che copre un periodo che si spinge fino al 2023. La novità più grande è naturalmente legata alle prime previsioni relative allo sviluppo delle reti 5G. Secondo Cisco, infatti, nel 2023 le reti 5G trasporteranno il 10% di tutto il traffico Internet mobile, offrendo una velocità di connessione media di 575 Mbit/s<sup>33</sup>.

Entro il 2023:

- A livello mondiale, la velocità di connessione in 5G sarà 3 volte superiore alla velocità media delle connessioni mobili (nel 2018); le connessioni 5G saranno il 10% nel mondo e il 14,8% in Italia.
- Il 73% degli italiani e il 66% della popolazione mondiale (5,3 miliardi di persone) saranno utenti di Internet.
- In Italia ci saranno 511 milioni di oggetti connessi e connessioni, 8,5 per persona; nel mondo ne conteremo 30 miliardi, 45% dei quali connessi su reti mobili.
- La velocità media delle connessioni in banda larga salirà da 46 Mbps a 110 Mbps. In Italia si parte da 24,5 Mbps e si arriverà a 75 Mbps di media.
- Nel mondo, il numero di *hotspot* che usano il Wi-Fi6 aumenterà di 13 volte tra il 2020 e il 2023, fino a diventare l'11% di tutti gli *hotspot* Wi-Fi pubblici del mondo.

Con sviluppi e *performance* di questo livello, il 5G permetterà di disporre di infrastrutture mobili più dinamiche, che potranno sostenere le applicazioni basate sull'intelligenza artificiale e sui nuovi sviluppi dell'IoT (veicoli a guida autonoma, *smart city*, servizi sanitari connessi, video immersivi).

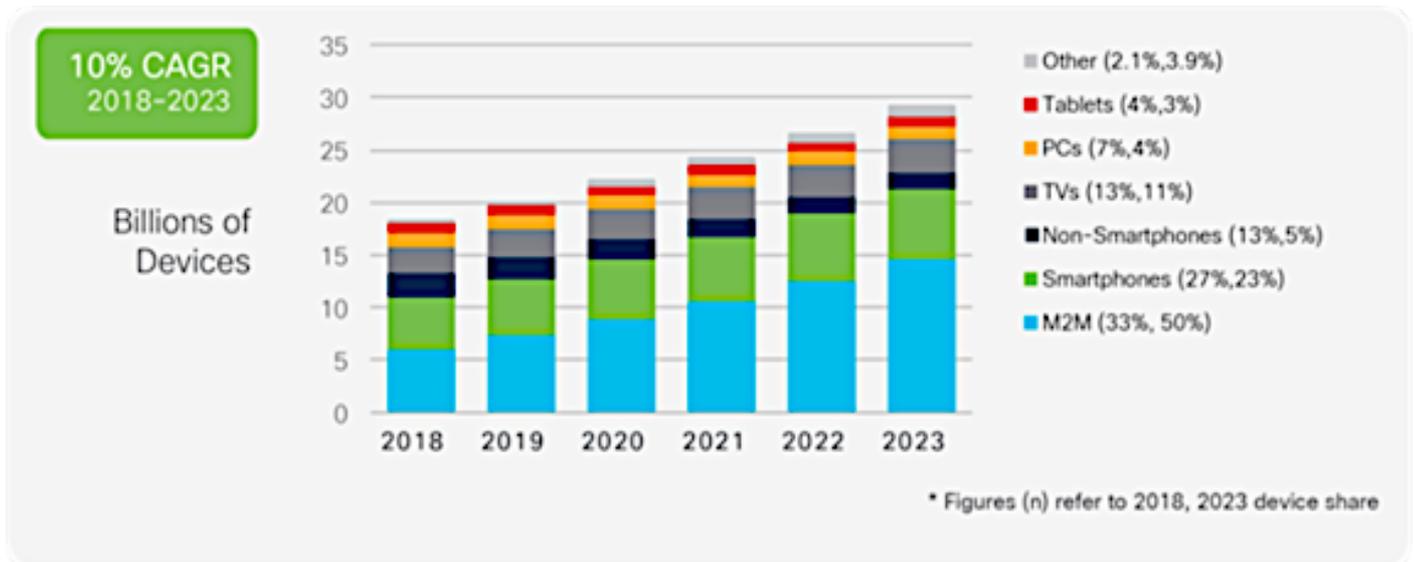
Si tratta di un nuovo *step* per l'evoluzione delle tecnologie mobili che nell'ultimo cinquantennio, ogni dieci anni circa, si sono rinnovate e hanno supportato richieste di banda sempre crescenti: da voce e testi fino ad arrivare oggi alla realtà aumentata e virtuale.

Che la domanda e le aspettative siano sempre crescenti, sia a livello aziendale sia tra i consumatori, lo dimostra il *trend* delle applicazioni di *social network*, *streaming* e *download* di video, strumenti per la produttività, *e-commerce* e *gaming*. Tali applicazioni continueranno a espandersi, tanto che nel 2023 le applicazioni scaricate dagli utenti sui loro *device* mobili saranno quasi 300 miliardi. In questo campo anche gli italiani non si risparmieranno, dato che si passerà dai 2,3 miliardi di applicazioni scaricate nel 2018 ai 2,8 miliardi nel 2023.

---

<sup>33</sup> Cisco annual internet report, 2018-2023, Cisco, 2020.

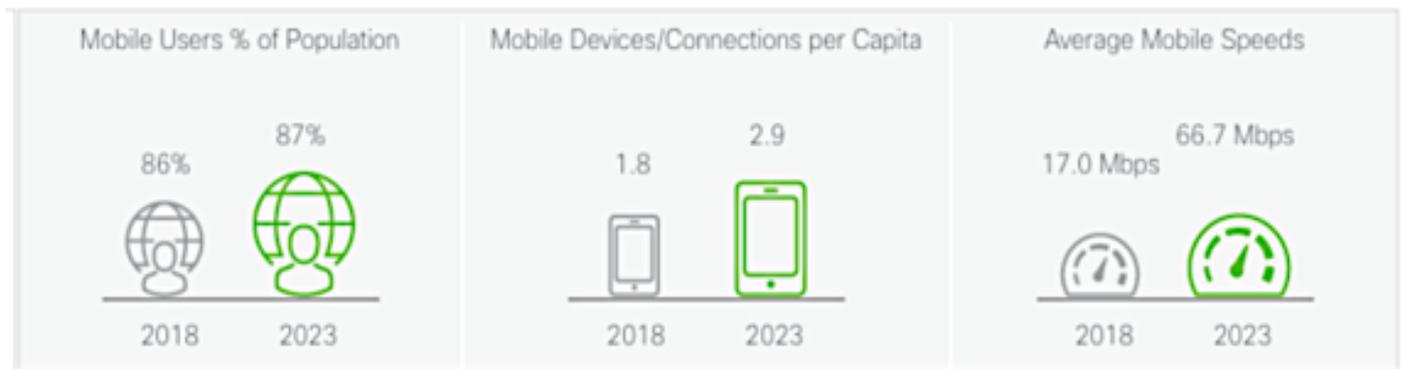
Grafico 19 - Trend e tipologia dei dispositivi connessi alla rete.



Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

A livello di stime globali, nel 2023 il 66% della popolazione mondiale sarà connessa a Internet, con una media di 3,6 dispositivi collegati a Internet pro-capite, per un totale di 30 miliardi di prodotti connessi. Di questi, ben il 50% sarà costituito non da *device* personali come *smartphone* o PC [Grafico 19], ma da dispositivi IoT che comunicheranno autonomamente con altri oggetti: macchine che parlano con macchine. Più nel dettaglio, Cisco prevede che il traffico M2M (*Machine to Machine*) sarà generato per il 48% da oggetti per la *Connected Home*, mentre la categoria che farà registrare la crescita maggiore sarà costituita dalle auto connesse, con un tasso di crescita annuale del 30% nel periodo 2018 - 2023.

Figura 20 – Previsioni di: popolazione connessa a Internet, connettività mobile, velocità di connessione.



Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

Venendo alle previsioni per l'Italia [Figura 20], nel 2023 il 73% della popolazione sarà connessa a Internet, con una media di 8,5 *device* connessi pro-capite, di cui 2,9 con connettività mobile, in crescita rispetto a 1,8 di media del 2018. La velocità di connessione *broadband* media sarà di 75,9 Mbit/s, mentre la velocità media delle reti mobili sarà di 66,7 Mbit/s.

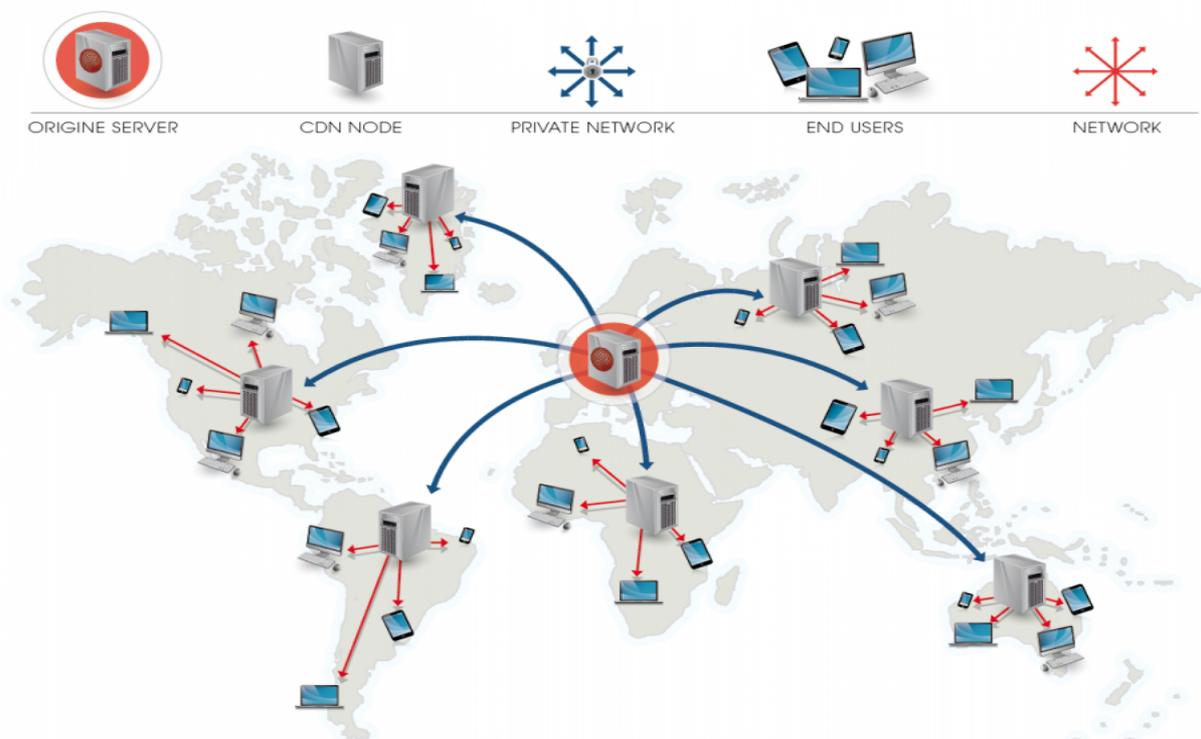
Le connessioni 5G costituiranno il 14,8% del traffico cellulare italiano, ma è interessante la stima della varietà di dispositivi connessi previsti da Cisco in Italia: il 71% dei 511 milioni di *device*, infatti, sarà costituito da prodotti di fascia *consumer*, in linea con il 72% del 2018, ma la quota degli *smartphone* si ridurrà dal 17% al 13%, mentre salirà dal 56% al 69% il numero di dispositivi M2M, quindi ben al di sopra della media mondiale.

# CAPITOLO 2: LE CONTENT DELIVERY NETWORK

## 2.1 Un po' di storia

Una rete CDN (*Content Delivery Network*) è una piattaforma di *server* altamente distribuita che aiuta a minimizzare il ritardo nel caricamento dei contenuti delle pagine *web* riducendo la distanza fisica e logica tra il *server* e l'utente [Figura 21]. Per fare ciò le CDN pongono i propri *server* all'interno dei POP (*Point of Presence*), ossia i punti di interconnessione fra i vari segmenti della rete Telco. In tal modo, gli utenti in tutto il mondo possono visualizzare gli stessi contenuti ad alta qualità senza rallentare i tempi di caricamento.

Figura 21 - Struttura di una Content Delivery Network (CDN)



Ad esempio, supponiamo di eseguire una campagna pubblicitaria e di pubblicizzare un servizio o prodotto tra milioni di potenziali clienti. Ci potremmo aspettare che un gran numero di clienti si precipiti sul sito dopo aver letto il *post*. Se si ha a che fare con *influencer* che hanno buoni tassi di coinvolgimento del pubblico, il volume di traffico può far registrare un picco ancora maggiore. Per tale motivo non vi è la certezza che il *server* di origine sia in grado di gestire questo picco di volume concentrato. In uno scenario del genere, le CDN possono aiutare a distribuire il carico tra i *server* perimetrali e tutti gli utenti riceveranno la risposta. Poiché solo una piccola parte delle richieste raggiungerà l'origine, i *server* non subiranno picchi di traffico massicci ed eventuali sovraccarichi. In assenza di una CDN, i *server* di origine dei contenuti devono rispondere a ogni singola richiesta degli utenti finali, il che si traduce in elevate richieste verso l'origine e un conseguente

carico/*stress* che può aumentare le probabilità di un guasto del *server* di origine in caso di picchi di traffico estremamente elevati o di un carico persistente. Rispondendo alle richieste degli utenti finali al posto dell'origine e da un'ubicazione fisica e di rete molto vicina a questi ultimi, una CDN distribuisce il traffico tra i *server*, migliorando la *web experience* con conseguenti vantaggi sia per il *provider* di contenuti che per gli utenti finali<sup>34</sup>.

Questa tecnologia è stata presentata per la prima volta nel 1995 dalla NEXUS International Broadcasting Association, un'organizzazione no-profit dedicata alla ricerca e allo sviluppo di tecnologie informatiche e telematiche nell'ambito del multimedia, con un'infrastruttura di rete per la distribuzione dei contenuti chiamata "World Director". Questa prima generazione di CDN fu rilevata dalla Wornex International, che tutt'ora sfrutta tale tecnologia per offrire ai propri clienti servizi di *hosting* ad alta velocità ed affidabilità tramite l'uso di una *Content Delivery Network* basata su una rete a bilanciamento globale.

In generale, l'evoluzione delle CDN può essere classificata in quattro generazioni:

1. Periodo di pre-formazione: prima dell'effettiva creazione delle CDN, le tecnologie e le infrastrutture necessarie erano in fase di sviluppo. Questo periodo è stato caratterizzato dall'ascesa delle *server farm*, dalla memorizzazione nella *cache* gerarchica, dai miglioramenti nei *server web* e dalla distribuzione dei *proxy* di memorizzazione nella *cache*. *Mirroring*, *caching* e *multihoming* sono tecnologie che hanno aperto la strada alla creazione e alla crescita delle CDN.
2. Prima generazione: le prime CDN si sono concentrate principalmente sulla distribuzione di contenuti dinamici e statici, poiché questi erano gli unici due tipi di contenuto sul *web*. Il meccanismo principale allora era la creazione e l'implementazione di repliche, metodi di *routing* intelligente e di *edge computing*. Le applicazioni e le informazioni sono state suddivise tra i vari *server*.
3. Seconda generazione: sono arrivate le CDN che si sono concentrate sullo *streaming* di contenuti audio e video, sui servizi di *Video-on-Demand* come Netflix e sui servizi di news. Questa generazione ha anche aperto la strada alla fornitura dei contenuti dei siti *web* agli utenti mobili e ha visto l'utilizzo di tecniche P2P e di *cloud computing*.
4. Terza generazione: si fa riferimento alla situazione attuale che si sta evolvendo con attività di ricerca e sviluppo. Possiamo aspettarci che le CDN in futuro saranno sempre più modellate per la comunità. Ciò significa che i sistemi saranno guidati da utenti medi e individui normali. L'auto-configurazione dovrebbe essere il nuovo meccanismo tecnologico, così come l'autogestione e la consegna autonoma dei contenuti. La qualità dell'esperienza (QoE) per gli utenti finali dovrebbe essere il motore principale in futuro.

---

<sup>34</sup> *Content Delivery Network, ecco che cos'è e quando usarlo*, 17 dicembre 2018. Articolo pubblicato su: NetworkDigital360.

Inizialmente le CDN si sono evolute per far fronte a pressioni sulla larghezza di banda, poiché la richiesta di *streaming* video era in crescita insieme al numero di fornitori di servizi CDN. Con i progressi della connettività e le nuove tendenze di consumo, il prezzo dei servizi CDN è diminuito, divenendo una tecnologia di mercato di massa. Inoltre, poiché il *cloud computing* è stato ampiamente adottato, le CDN hanno svolto un ruolo chiave in tutti i livelli delle operazioni aziendali. Sono fondamentali per modelli come SaaS (*Software as a service*), IaaS (*Infrastructure as a service*), PaaS (*Platform as a service*) e BPaaS (*Business Process as a service*).

## 2.2 L'avvento di Akamai

Ad oggi il ruolo di *leader* indiscusso in questo settore è ricoperto dalla Akamai Technologies. Era il 1998 quando Lewin insieme ad altri 4 soci fonda Akamai Technologies, una delle meno note e più importanti aziende coinvolte nella crescita della rete che ha contribuito molto allo sviluppo di Internet, diventando uno dei principali attori sul mercato per le reti di consegna dei contenuti (CDN). La grande intuizione di Lewin e colleghi fu capire prima di molti altri che la rete aveva bisogno di un sistema di ottimizzazione specifico per ottenere la massima velocità e la massima capacità di trasporto nella distribuzione delle informazioni. Attraverso la creazione di un algoritmo estremamente sofisticato capace di modellizzare i flussi di *bit* all'interno della rete, essi resero tutto ciò possibile. Il sistema sviluppato da Lewin aveva lo scopo di ottimizzare i flussi di dati evitando il sovraccarico dei *server* centrali (e di tutti gli altri apparati collegati, come *server*, *switch* e *router*) quando, ad esempio, un contenuto *web* veniva richiesto contemporaneamente da più parti del mondo. Il sistema funzionava grazie ad alcuni meccanismi di ottimizzazione costruiti ai bordi dell'infrastruttura della rete che fungevano sia da memoria tampone sia da regolatori del traffico di informazioni. Questi meccanismi creavano delle copie dei contenuti, che venivano allocate ai bordi dell'infrastruttura della rete e permettevano di massimizzare le *performance* ed impedire il sovraccarico dei *server* centrali quando, per esempio, una pagina *web*, una canzone digitale di uno *store online*, un film o un videogioco venivano richiesti da più utenti contemporaneamente in parti diverse del pianeta. Una parola stava prendendo forma in quel periodo per definire il lavoro di ottimizzazione e organizzazione dei flussi dei dati fatta per conto terzi: CDN, *Content Delivery Network*.<sup>35</sup>

Akamai e poche altre aziende avevano infatti intuito che il futuro di Internet, basato su protocolli che consentivano la circolazione dei pacchetti di dati in modo quasi schizofrenico attraverso un continuo zigzagare di percorsi diversi, richiedeva un meccanismo che creasse ordine per ottenere il massimo della velocità ma anche della capacità di trasporto possibile. Anziché ricorrere a un tipo di rete diversa, organizzata in maniera gerarchica e strutturata, l'idea di Lewin era stata quella di costruire ai bordi della rete alcuni meccanismi di ottimizzazione, che facessero sia da memoria tampone che da *relè* del traffico. L'algoritmo, estremamente sofisticato, sceglieva quali pacchetti di *bit* inviare verso quali blocchi di memoria tampone e poi dove trasferirli e con quali *relè*. Tuttavia l'algoritmo creato da Lewin faticava a prendere quota: mancavano i clienti.

---

<sup>35</sup> Breve storia delle CDN, blog, CRITICALCASE.

Quando si facevano i conti tra i guadagni e le spese in ricerca e soprattutto in macchinari necessari al funzionamento dell'azienda, il saldo era negativo. Lewin morì a 31 anni a bordo del volo AA 11 durante gli attacchi dell'11 settembre 2001 e proprio nei giorni successivi a questo evento ci fu il trionfo del suo algoritmo. Dopo l'11 settembre, infatti, la rete fu sottoposta a uno dei test più duri per quanto riguarda la sua capacità di resistere ai carichi di lavoro: decine, centinaia di milioni di persone nelle ore dopo gli attentati cercarono informazioni sugli eventi, mentre la capacità dei *server* di base dell'epoca era portata rapidamente alla saturazione. Ci furono numerose disfunzioni e *blackout*, incapacità da parte dei nodi della rete di gestire il carico di richieste contemporanee. Ma se l'infrastruttura tecnologica dell'epoca nel complesso è stata in grado di rispondere al sovraccarico di richieste, il merito è stato certamente anche di Lewin e dei suoi collaboratori.

Oggi Akamai è sopravvissuta al suo fondatore ed è uno dei principali attori nel mercato delle CDN, le reti per la consegna di contenuti, ma non è certamente il solo. Decine di aziende (CDNetworks, CloudFlare, Limelight Networks, MaxCDN, EdgeCast Networks, Mainstreaming oltre alle CDN di Amazon, Google e Microsoft) stanno costruendo uno degli snodi più importanti per la crescita e il funzionamento di Internet.

Il lavoro che compiono dietro le quinte è fondamentale: gestiscono i flussi di *bit* che compongono il 90% del traffico della rete con l'obiettivo di abbattere i tempi di attesa e ridurre i sovraccarichi. Servono per gestire il traffico della maggior parte dei servizi di *cloud computing*, permettono di ottimizzare la dimensione dei filmati, dell'audio e delle immagini inviate verso i dispositivi mobili, svolgono un ruolo fondamentale nella sicurezza dei dati attraverso la rete e nella disponibilità dei servizi per gli utenti, senza contare il ruolo strategico che giocano per la televisione. In modo totalmente trasparente per l'utente, dietro le quinte, le CDN si fanno carico di prendere il flusso di *bit* che compongono le immagini di una partita di calcio e di replicarlo in maniera strategica in decine di punti diversi della rete, reindirizzando a questi *relè* le richieste da parte degli utenti senza che questi ultimi possano rendersene neanche conto. Il tutto in pochi centesimi di secondo<sup>36</sup>.

I servizi CDN sono essenziali per le aziende che si occupano della fornitura di contenuti agli utenti, in particolare per realtà che si occupano di:

- *Delivery* di contenuti di siti *web*.
- Diffusione e trasmissione internazionale di news.
- *Social media* che devono fornire contenuti multimediali agli utenti.
- Applicazioni di intrattenimento come Skygo e Netflix che forniscono contenuti *web* ad alta definizione in tempo reale o *On-Demand*.
- Piattaforme di *e-commerce* con milioni di clienti.
- *Gaming* con contenuti grafici a cui accedono simultaneamente utenti distribuiti geograficamente.

---

<sup>36</sup> Dini Antonio, *L'avventurosa storia delle CDN*, 3 maggio 2016, articolo pubblicato su: [LINK](#).

L'aumento continuo del numero di aziende che si spostano *online* e di utenti in ogni parte del mondo che utilizzano abitualmente Internet per fare acquisti, connettersi e condividere contenuti, pone i *provider* di fronte a sfide sempre più diversificate, come distribuire tipi diversi di contenuti, adattarli a molteplici tipologie di dispositivi (rilevamento dei dispositivi) e proteggere i dati e la presenza *online* dei propri utenti finali. Tutte queste aziende devono garantire l'accelerazione della distribuzione dei contenuti, la disponibilità dei servizi, la scalabilità delle risorse e la sicurezza delle applicazioni *web*. È qui che i servizi CDN garantiscono un vantaggio competitivo<sup>37</sup>.

### 2.3 Il ruolo strategico della televisione nel mercato delle CDN

La televisione è un'area altamente strategica perché il video in alta definizione soffre del problema della capacità di trasmissione: le reti si saturano facilmente e i *server* possono rispondere alle richieste da parte degli utenti anche con dieci, venti, trenta secondi di ritardo. Le conseguenze commerciali sono terribili.

La clessidra che gira e il pallone da spiaggia che ruota con i colori dell'arcobaleno sono metafore visive per indicare che "il servizio richiede tempo per essere erogato". Vengono interpretate dai consumatori come un segnale di poca banda passante, di lentezza, ma in realtà rappresentano un problema completamente diverso: un eccesso di carico di lavoro, che satura la capacità di risposta del *server* centrale.

Il "rifiuto di prestare il servizio" (*denial of service*) è alla base di moltissimi dei problemi informatici di Internet, anche di sicurezza (vedi caso Dazn, ritardo Skygo rispetto al *live*).

Per questo la distribuzione capillare e automatica su decine, centinaia di punti strategici, consente di ovviare al problema e ridurre il tempo di attesa, quella che gli americani chiamano la *spinning beach ball of death*, l'attesa mortale (mortale perché l'utente percepisce il sistema come se non si potesse più riavviare) capace di azzerare la presenza di utenti attivi. Dieci secondi di attesa scoraggiano infatti due terzi degli utenti e, se il ritardo sale a venti secondi, il servizio diventa deserto. Le CDN mirano ad abbattere le attese e a ricondurre i sovraccarichi a tempi più accettabili, attorno al secondo.

Dopotutto, il picco è sempre stato uno dei grandi problemi della tecnologia; problemi che però hanno potuto generare anche opportunità. Un esempio: Amazon, che ha costruito il suo modello di *business* sulla capacità logistica delle sue consegne e anche sulla capacità di calcolo dei suoi *server*, ha dovuto configurare la sua infrastruttura tecnologica in modo che potesse resistere ai picchi più estremi di richieste di acquisti *online*, tipicamente per il *Black Friday* e il periodo natalizio. Picchi che comportano un'extra-capacità poi inutilizzata per tutto il resto dell'anno. Per questo l'azienda, e in particolare il suo responsabile della tecnologia Werner Vogels, è considerata la madre del *cloud computing*, cioè di un modello di distribuzione delle risorse di calcolo intese come servizio e non più come prodotto.

---

<sup>37</sup> *Che cos'è una CDN?*, articolo di Akamai.

L'idea di Amazon è stata di realizzare una rete privata e affittare la capacità di calcolo e la memoria dei suoi *server* nei periodi di scarso utilizzo. Un'idea talmente buona che ha poi preso piede consentendo a Jeff Bezos di fondare Amazon Web Services (AWS), divisione autonoma del colosso dell'*e-commerce* che è la capofila di una serie di aziende che stanno dando una forte spinta a questo modello complesso ma estremamente completo di fornitura dei servizi informatici<sup>38</sup>. Per le aziende clienti questo ha voluto dire poter utilizzare una grande capacità di calcolo senza dovere fare i relativi investimenti. Niente spese di capitale, dunque, ma solo il pagamento di un servizio a consumo, che è contabilizzato oltretutto come spesa operativa. Il passaggio da *Capex* a *Opex*, oltre alla minore entità della spesa, ha comportato il vero cambiamento per le grandi aziende.

Il minor costo e la maggiore flessibilità si pagano però con il rischio che il servizio non sia sempre disponibile, sia per cattivo funzionamento dei *server* sia per problemi di intasamento della rete. Per servizi relativamente secondari e a basso impatto, come la posta elettronica (solitamente per le grandi aziende in cima alla lista delle attività da esternalizzare), lo stop di qualche minuto può non essere un problema. Per chi, come ad esempio le *startup* nel settore dello *streaming* di contenuti, vive di risposte in tempo reale, l'incapacità di garantire un servizio continuo fa la differenza tra la possibilità di restare in piedi e il fallimento.

Ecco perché negli ultimi due anni il ruolo dei fornitori di servizi di CDN è diventato sempre più strategico e neanche i *big* del settore riescono a ovviare a questo problema facendo da soli. Gli algoritmi altamente ottimizzati e testati da anni sul campo da parte degli specialisti sono, infatti, impossibili da replicare con la medesima efficienza e, inoltre, lo sviluppo di centinaia di punti di accesso che facciano da *relè* al traffico di rete è semplicemente troppo costoso da realizzare e complesso. Per questo aziende come Akamai hanno clienti del calibro di Apple, Microsoft, la Bbc con il suo iPlayer, *network* televisivi in tutto il mondo (da Mtv alla Espn, dalla Nbc sport alla Cina Central Television), catene alberghiere come Hilton, la Nasa, colossi *hi-tech* come Adobe, Ibm, Yahoo e decine di altre aziende grandi e piccole.

---

<sup>38</sup> AWS ha la marginalità più elevata tra tutti i *business* di Amazon.

## 2.4 Come funziona una CDN?

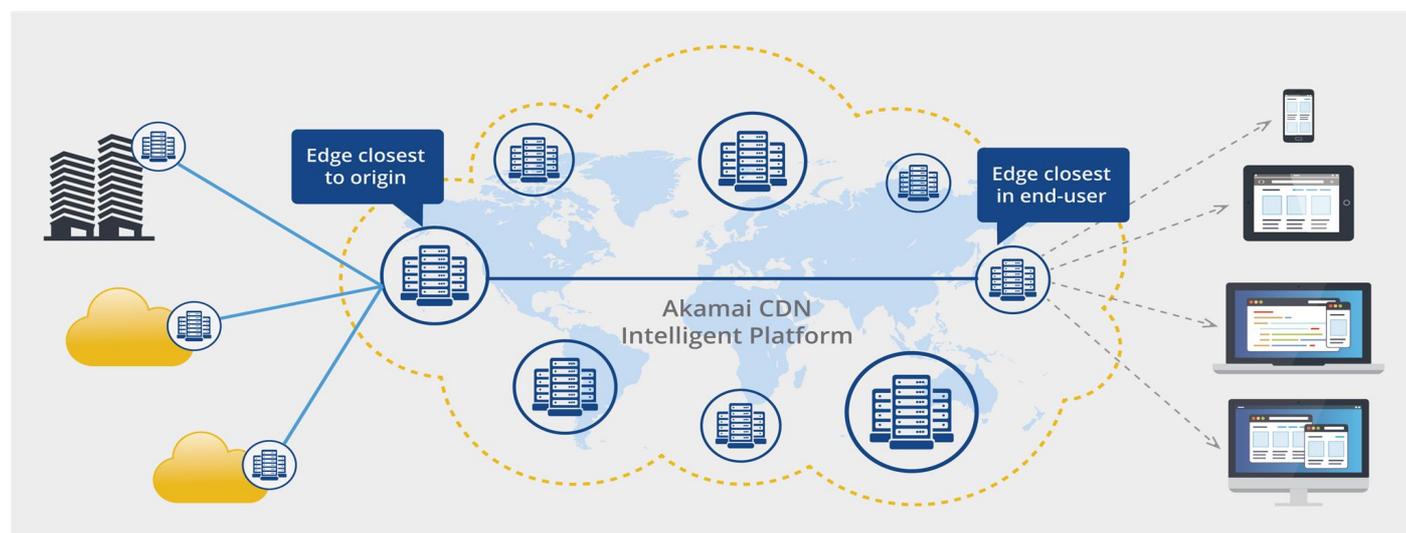
Più della metà del traffico in Internet viene gestito da una rete per la distribuzione dei contenuti (CDN). L'obiettivo della rete CDN è quello di incrementare la velocità di un sito *web* riducendo, al contempo, la latenza, ossia il ritardo tra l'inoltro di una richiesta su una pagina *web* ed il completamento del caricamento della pagina sul dispositivo in uso. Questo risultato si ottiene riducendo la distanza fisica che deve compiere la richiesta. È importante innanzitutto effettuare una distinzione tra:

- Distanza fisica: distanza tra utente ed il POP/*server* a lui più vicino.
- Distanza logica: percorso effettuato dalla richiesta dell'utente per accedere ad un contenuto (può essere ridotta aumentando numero dei POP, *Edge*).

Se, ad esempio, un visitatore della pagina *web* negli Stati Uniti desidera visualizzare i contenuti originati da un *server* in Inghilterra, risconterà tempi di caricamento molto lunghi se la richiesta deve compiere tutto il tragitto attraversando l'Atlantico. Per risolvere questo problema, la rete CDN memorizza nella *cache* una versione dei contenuti del sito *web* in più aree geografiche del mondo e le pone all'interno dei PoP nella rete dei Telco. I PoP contengono propri *server* di *caching*, che si occupano di consegnare i contenuti all'utente. Gli *User-Agent*, sostanzialmente dei dispositivi che eseguono i *browser web*, effettuano le richieste dei contenuti per il *rendering* di pagine *web*, quali *file* HTML, CSS, JavaScript e di immagini.

Nella maggior parte delle CDN, ogni richiesta di contenuti comporta la mappatura dell'utente finale rispetto a un *server* CDN in posizione ottimale, che risponde restituendo la versione dei *file* richiesti precedentemente memorizzata nella *cache*. Nel caso in cui i *file* non vengano individuati, il contenuto viene cercato sugli altri *server* della piattaforma CDN e la risposta viene inviata all'utente finale. Quando il contenuto non è disponibile o risulta obsoleto, la CDN agisce da *proxy* inviando la richiesta al *server* di origine e successivamente memorizzando il contenuto recuperato per eventuali richieste future.

Figura 22 - Struttura della piattaforma di CDN dall'origine all'end-user.



Fonte: Akamai

Le CDN, quindi, funzionano riducendo la distanza fisica e logica tra l'utente e l'origine (un *server web* o un'applicazione). Si tratta di una rete di *server* distribuita a livello globale che memorizza il contenuto molto più vicino all'utente rispetto all'origine [Figura 22]. Le CDN consentono ai *server* periferici di precaricare i contenuti in anticipo. Ciò garantisce che i dati che si vogliono fornire siano archiviati in tutti i *data center* CDN. Per capire meglio il funzionamento delle CDN è utile esaminare come un utente accede ai contenuti da un sito *web* con e senza CDN<sup>39</sup>.

## Senza CDN

Quando un utente accede al sito *web* nel *browser* stabilisce una connessione simile a quella nella figura 23. Il nome del sito *web* si risolve in un indirizzo IP attraverso il DNS locale (ossia il sistema che regola la traduzione dei nomi dominio dei siti Internet in indirizzi IP) o LDNS (come il *server* DNS fornito dall'ISP o un *server* di risoluzione DNS pubblico). Se il DNS o LDNS non è in grado di risolvere l'indirizzo IP, richiede in modo ricorsivo la risoluzione ai *server* DNS a monte. Se anche questo non funzionasse, la richiesta potrebbe passare al *server* DNS autorevole. Questo *server* DNS risolve l'indirizzo e lo restituisce all'utente.

Figura 23 - Connessione stabilita da un utente quando accede ad un sito web.



Fonte: CDNetworks

Quindi, a questo punto, il *browser* dell'utente si collega direttamente all'origine e scarica il contenuto del sito *web*. Ogni richiesta successiva viene servita direttamente dall'origine e le risorse statiche vengono memorizzate nella *cache* locale sul dispositivo dell'utente. Se un altro utente da una posizione simile o diversa tenta di accedere allo stesso sito, eseguirà la stessa sequenza. Ogni volta le richieste degli utenti raggiungeranno l'origine e l'origine risponderà con il contenuto. Ogni passaggio lungo il percorso aggiunge un ritardo o latenza. Se l'origine si trova lontano dall'utente, i tempi di risposta subiranno una latenza significativa, offrendo un'esperienza utente scadente [Figura 24].

<sup>39</sup> *What is a CDN?* Fonte: <https://www.cdnetworks.com/>

Figura 24 - Come un utente accede a un contenuto senza CDN, maggiore è la distanza maggiore è la latenza.

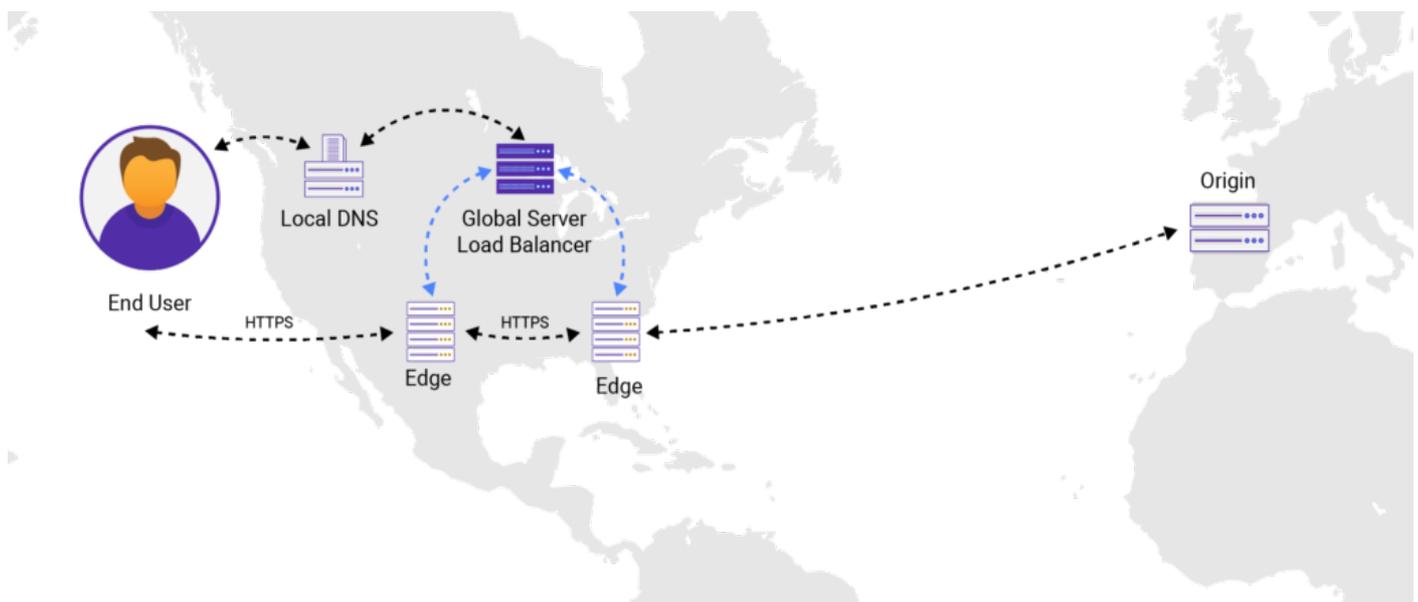


Fonte: CDNetworks

### Con CDN

In presenza di CDN, invece, il processo è leggermente diverso. Quando le richieste DNS avviate dall'utente vengono ricevute dal suo LDNS, esso inoltra le richieste a uno dei *server* DNS della CDN. Questi *server* fanno parte dell'infrastruttura *Global Server Load Balancer* (o "GSLB"). GSLB è un'infrastruttura che aiuta con la funzionalità di bilanciamento del carico l'intera rete Internet e tiene traccia delle informazioni su tutte le risorse disponibili e sulle loro prestazioni. Con questa conoscenza, il GSLB risolve la richiesta DNS utilizzando l'indirizzo *edge* con le migliori prestazioni, solitamente in prossimità dell'utente. Un programma di bilanciamento del carico globale, infatti, invia una richiesta a un *server* che si trova più vicino al *client*, diminuendo la latenza e migliorando le prestazioni. All'*edge* è presente un insieme di *server* che memorizzano nella *cache* il contenuto *web* e lo distribuiscono [Figura 25].

Figura 25 - Come un utente accede ad un contenuto con CDN.



Fonte: CDNetworks

Dopo che la risoluzione DNS è stata completata, l'utente effettua la richiesta HTTPS all'*edge*. Quando il perimetro/bordo riceve la richiesta, i *server* GSLB aiutano i *server* perimetrali a inoltrare le richieste seguendo il percorso ottimale verso l'origine. A questo punto i *server* perimetrali recuperano i dati richiesti, li consegnano all'utente finale e li archiviano localmente (nei POP). Tutte le successive richieste degli utenti verranno servite dal set di dati locale senza dover interrogare nuovamente il *server* di origine. Il contenuto così archiviato nell'*edge* può essere consegnato anche se l'origine non è disponibile per qualsiasi motivo.

È, però, importante effettuare la distinzione tra due tipi di contenuti:

- **Contenuto statico:** rappresenta la gran parte del traffico *web* prima dell'avvento del video. Si tratta di risorse che non devono essere generate, elaborate o modificate prima di essere fornite agli utenti finali. Queste potrebbero essere immagini o altri *file* multimediali, *file* binari di ogni tipo o parti statiche di un'applicazione come HTML, CSS, librerie JavaScript o anche JSON, HTML o qualsiasi tipo di risposta dinamica che non cambia spesso. Se il contenuto è statico è possibile precargarlo in anticipo, come accennato in precedenza. Quindi, quando è necessario invalidare tale contenuto e rimuoverlo dai *server* periferici, è possibile eliminare i percorsi desiderati.
- **Contenuto dinamico:** si fa riferimento a contenuti che non possono essere memorizzati nella *cache* all'*edge* a causa della loro natura dinamica. Se ad esempio prendiamo in considerazione un'applicazione WebSocket, che ascolta gli eventi da un *server* o un *endpoint* API la cui risposta è diversa, a seconda delle credenziali, della posizione geografica o di altri parametri, è difficile sfruttare il meccanismo della *cache* sul bordo della rete in un modo simile alla memorizzazione nella *cache* di un contenuto statico. In alcuni casi, una più stretta integrazione tra le applicazioni e le CDN può aiutare; tuttavia, dovrebbe essere utilizzato qualcosa di diverso dalla memorizzazione nella *cache*. Per l'accelerazione dinamica, viene utilizzata l'infrastruttura di rete ottimizzata di CDN e algoritmi di *routing* di richiesta/risposta avanzati.

### **Come funziona il CDN Caching?**

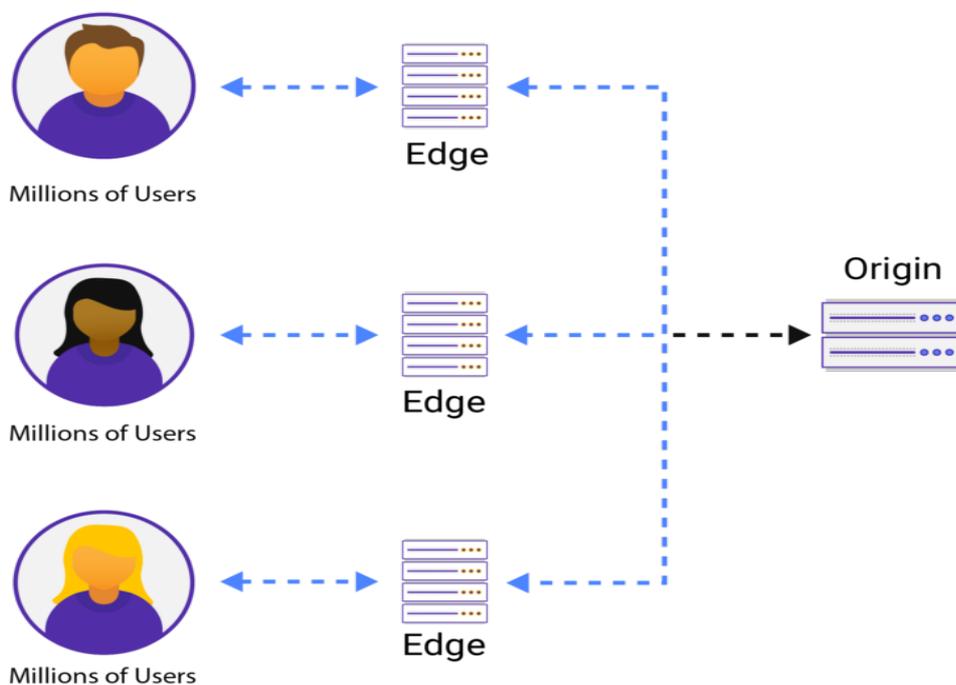
La memorizzazione nella *cache* CDN è una parte cruciale di ciò che fa funzionare le reti di distribuzione dei contenuti. Essa consiste nel processo di archiviazione di una copia dei *file* consegnati a un utente per la prima volta e di riutilizzo della copia archiviata per le richieste successive, invece dei *file* originali. In una rete CDN, i *server* perimetrali sono il luogo in cui i dati vengono memorizzati nella *cache*. La memorizzazione nella *cache* CDN funziona all'incirca secondo i seguenti passaggi:

1. Un utente finale richiede per la prima volta *asset* statici sulla pagina *web*.
2. Gli *asset* vengono recuperati dal *server* di origine e, una volta consegnati, vengono archiviati nel *server* di *cache edge* PoP vicino all'utente finale.

3. Quando lo stesso utente richiede le stesse risorse la volta successiva, le richieste non vanno al *server* di origine. Esse vanno invece ai *file* memorizzati nella *cache* dal *server* PoP per verificare se le risorse archiviate sono ancora disponibili e consegnarle all'utente. Se non sono disponibili o il *server* di memorizzazione nella *cache* non ha ancora memorizzato nella *cache* le risorse, la richiesta viene inviata nuovamente al *server* di origine.

Una volta che le risorse statiche sono state memorizzate nella *cache* su tutti i *server* CDN per una particolare posizione, tutte le successive richieste dei visitatori del sito *web* per le risorse statiche verranno consegnate da questi *server* perimetrali anziché dall'origine, riducendo così il carico all'origine e migliorando la scalabilità per tutti i visitatori che sono serviti da quella specifica *cache* [Figura 26].

Figura 26 - Consegna di risorse statiche agli utenti attraverso i server perimetrali e non l'origine.



Fonte: CDNetworks

## 2.5 I diversi tipi di CDN

Per quanto riguarda le diverse tipologie di CDN, vi sono sostanzialmente due classificazioni:

1. *Peer-to-peer* (P2P) VS CDN private.
  2. CDN *push* VS CDN *pull*.
- *Peer-to-peer* (P2P): Le CDN di rete P2P coinvolgono singoli sistemi che sono stati aperti per consentire a un *server* di scaricare dei *file*. Il *server* che lo abilita è chiamato *tracker*, sebbene possa anche trattarsi di una piccola rete di *server*. Ad esempio, prendiamo in considerazione una piattaforma di condivisione *file* come BitTorrent in cui un utente cerca *file* specifici da scaricare. Invece di scaricarli da un singolo *server*, il *tracker* cercherà in più computer che contengono lo stesso *file* e scaricherà parti diverse del *file* da ciascun sistema. Per questo motivo i CDN P2P hanno una struttura molto decentralizzata, che può causare rischi per la sicurezza.
  - CDN private (*peering*): Il modello di CDN privata o di *peering* è caratterizzato da una situazione in cui una società è proprietaria della rete e controlla i *server* in tutta la loro area di copertura. Invece di fare affidamento su un modello decentralizzato, le CDN *peering* controllano i loro *server* che ospitano il contenuto di un sito *web*. Quando i visitatori accedono al sito *web*, i *file* verranno scaricati dal *server* che fisicamente è più vicino all'utente.
  - *Push* CDN: Si tratta di CDN in cui l'utente o il *server* primario invia il contenuto alla CDN. Funziona essenzialmente come un *server* secondario in cui è l'utente che carica i contenuti direttamente sulla CDN. Gli utenti possono specificare quali contenuti caricare e quando questi devono essere aggiornati o rimossi (perché ad esempio vecchi). Questo tipo di CDN è utile quando si desidera controllare il traffico, e come questo viene utilizzato, dato che i caricamenti devono avvenire solo in caso di modifica.
  - *Origin pull* CDN: Nelle CDN *origin pull*, l'utente non invia i *file* alla CDN, ma avviene il contrario. La CDN estrae il contenuto dal *server* di origine dove viene salvato dal proprietario, prima di consegnarlo all'utente finale. Rispetto alle CDN *push*, le CDN *pull* di origine possono essere più lente e meno flessibili in quanto può esserci una certa ridondanza nel traffico, specialmente quando i *file* vengono richiesti prima che vengano apportate le necessarie modifiche e aggiornamenti. Il vantaggio dell'utilizzo delle CDN *pull* di origine è che sono più facili da configurare e riducono al minimo lo spazio di archiviazione.

## 2.6 Vantaggi nell'utilizzo di una CDN

A seconda delle dimensioni, del *business* e delle esigenze di una azienda, i vantaggi di una CDN possono essere suddivisi in quattro diversi aspetti:

1. Miglioramento dei tempi di caricamento della pagina del sito *web* (minor latenza).

Spostando e archiviando i contenuti del sito *web* più vicino agli utenti, utilizzando un *server* CDN nelle vicinanze, i visitatori sperimentano tempi di caricamento delle pagine *web* più rapidi ed un'esperienza di navigazione migliore. Come già analizzato in precedenza, i visitatori sono generalmente più inclini a fare *click* su un sito *web* veloce ed evitare quei siti con un tempo di caricamento della pagina elevato. Un tempo di caricamento elevato può anche influire negativamente sul posizionamento della pagina *web* sui motori di ricerca. Quindi avere una CDN può ridurre la frequenza di rimbalzo da parte dell'utente e aumentare la quantità di tempo che le persone trascorrono sul sito. In altre parole, un sito *web* che si carica rapidamente manterrà più visitatori e più a lungo.

2. Riduzione dei costi per la larghezza di banda.

Ogni volta che un *server* di origine risponde a una richiesta, la larghezza di banda viene consumata. I costi del consumo di larghezza di banda rappresentano una spesa importante per le aziende. Attraverso il *caching* e altre ottimizzazioni, le CDN sono in grado di ridurre la quantità di dati che un *server* di origine deve fornire, riducendo così i costi di *hosting* per i proprietari di siti *web*.

3. Aumento della disponibilità e della ridondanza dei contenuti.

Grandi quantità di traffico *web* o guasti all'*hardware* possono interrompere il normale funzionamento del sito *web* e causare tempi di inattività. Grazie alla loro natura distribuita, le CDN possono gestire più traffico *web* e resistere a guasti *hardware* meglio di molti *server* di origine. Inoltre, se uno o più *server* CDN vanno *offline* per qualche motivo, altri *server* operativi possono raccogliere il traffico *web* e mantenere il servizio ininterrotto.

4. Miglioramento della sicurezza del sito *web*<sup>40</sup>.

Lo stesso processo con cui le CDN gestiscono i picchi di traffico può essere ideale per mitigare gli attacchi *Denial of Service* (DDoS). Si tratta di attacchi in cui gli attori malintenzionati saturano un'applicazione o i *server* di origine inviando una quantità enorme di richieste. Quando il *server* si arresta a causa del volume, il tempo di inattività può influire sulla disponibilità del sito *web* per i clienti.

---

<sup>40</sup> Vedi appendice sulla sicurezza.

Una CDN agisce essenzialmente come una piattaforma di protezione e mitigazione degli attacchi DDoS attraverso GSLB (*Global Server Load Balancing*) e *server* perimetrali che distribuiscono il carico equamente su tutta la capacità della rete. Poiché la CDN è distribuita ai margini della rete, funge da barriera virtuale con un'elevata sicurezza contro gli attacchi ad un sito *web* e alle applicazioni. L'infrastruttura sparsa e la posizione *on-edge* rende inoltre una CDN ideale per bloccare i *flood* DDoS. Poiché questi attacchi devono essere mitigati al di fuori dell'infrastruttura di rete principale, la CDN li elaborerà su diversi PoP in base alla loro origine, prevenendo la saturazione del *server*. Le reti CDN possono anche generare, gestire e rinnovare automaticamente i certificati. Infatti, possono aiutare a proteggere un sito fornendo *Transport Layer Security* (TLS)/*Secure Sockets Layer* (SSL) che garantiscono un elevato *standard* di autenticazione, crittografia e integrità. Si tratta di certificati che garantiscono il rispetto di determinati protocolli nel trasferimento di dati tra un utente e un sito *web*. Quando i dati vengono trasferiti su Internet, diventano vulnerabili all'intercettazione da parte di malintenzionati. Questo viene risolto crittografando i dati attraverso l'utilizzo di un protocollo che solo il destinatario previsto può decodificare. TSL e SSL sono protocolli che crittografano i dati inviati su Internet. È possibile comprendere se un sito *web* utilizza la certificazione TLS/SSL se inizia con `https://` invece che con `http://`, suggerendo che è abbastanza sicuro per la comunicazione tra un *browser* e un *server*.

## 2.7 La sfida attuale: le CDN nello *streaming*

Lo *streaming live* è il processo mediante il quale i dati sotto forma di video, audio e altri *media* di alta qualità vengono trasmessi dai creatori agli utenti attraverso Internet in tempo reale. Invece di scaricare un *file* video di grandi dimensioni prima di riprodurlo, lo *streaming live* consente agli utenti di scaricare il *file* un po' alla volta e riprodurlo in tempo reale. In sostanza, il *live streaming* è la tecnologia che consente di creare, condividere e guardare video *online* in tempo reale. Può essere fruito su Internet con dispositivi collegati, come *laptop*, telefono, *tablet*, o con un'applicazione che consenta lo *streaming live*. Si pensi ad esempio alle applicazioni e alle funzionalità di consumo popolari come Instagram Live, Facebook Live, Twitch e Tik Tok che consentono di visualizzare i contenuti video *online* creati dagli utenti mentre li trasmettono in diretta. Anche i *file* multimediali come i video di YouTube vengono trasmessi in *streaming* tecnicamente, ma non generalmente in *live streaming* poiché la trasmissione non deve avvenire in tempo reale. Non è solo il contenuto visualizzabile pubblicamente che viene utilizzato nello *streaming* video in diretta, si possono impostare anche eventi privati e accessibili solo a utenti selezionati, come nel caso di strumenti di videoconferenza come Zoom o Teams. L'ascesa delle tecnologie di *live streaming* ha trasformato e sta continuando a trasformare l'industria dei *media* e dell'intrattenimento. Dagli sport professionistici ai notiziari, dalle piattaforme e dalle applicazioni dei *social media* ai videogiochi, quasi ogni forma di *media* e intrattenimento oggi coinvolge alcuni aspetti dello *streaming* video in diretta.

## Come funziona una CDN di *live streaming*?

Lo *streaming live* funziona inviando contenuti su Internet in tempo reale senza registrare interi *file* e archivarli. Se facciamo riferimento allo *streaming* video di alta qualità, ci sono cinque passaggi tra la creazione del contenuto e la fruizione dello stesso da parte dell'utente finale.

### 1. Acquisizione video.

Innanzitutto, il creatore di contenuti acquisisce i dati grezzi o le informazioni visive utilizzando una fotocamera. I dati sono rappresentati in binari 1 e 0 nel dispositivo.

### 2. Segmentazione.

Questa è la fase dove il *file* video viene suddiviso in parti più piccole della durata di pochi secondi. Allo stato attuale, i *file* video sono di dimensioni molto più grandi e anche il *download* di interi *file* richiede molto tempo. Suddividerli in segmenti aiuta a trasmettere in *streaming* l'intero video un po' alla volta.

### 3. Compressione e codifica.

Ciascuno dei segmenti è compresso e codificato. La compressione rimuove le informazioni visive ridondanti come uno sfondo che non cambia nel video. Ciò semplifica il *rendering* dei soli fotogrammi in movimento nel video prima dello *streaming*. La codifica è un processo necessario per convertire i dati in un formato compatibile con la varietà di dispositivi su cui l'utente finale riproduce il contenuto. Ad esempio H.264, HEVC, VP9 e AV1 sono alcuni dei formati popolari in cui vengono codificati i video.

### 4. Distribuzione dei contenuti e *cache* CDN.

Successivamente, il video segmentato, compresso e codificato viene distribuito agli utenti finali. Quando l'utente finale accede a un sito *web* o riproduce un video, il suo dispositivo (*client*) invia una richiesta al *server* di origine per recuperare questi *file*. Ovviamente, se gli utenti si trovano nelle immediate vicinanze del *server* o all'interno di una regione vicina, questo non genera problemi e i *file* video vengono riprodotti in *streaming* senza troppe difficoltà con un'adeguata QoE. Infatti, se le visualizzazioni di un determinato contenuto sono ridotte e non sono ampiamente distribuite, il singolo *server* può trasmettere in *streaming* a tutti gli utenti e non risulta necessario introdurre più elementi nel flusso di lavoro di *streaming*. Ma quando gli utenti sono dispersi in un'area geografica più ampia, in alcuni casi in paesi diversi, il tempo di andata e ritorno dal *server* per fornire il contenuto può essere più lungo, con conseguenti ritardi o latenza. Ciò si traduce in un'esperienza per l'utente al di sotto della media e diversificata tra i consumatori del video. L'utilizzo di una rete CDN risolve questo problema dato che memorizza nella *cache* della rete distribuita dei *server* lo *streaming* del contenuto. Il *server* CDN più vicino a un particolare utente finale si occuperà di consegnare il contenuto a quell'utente.

## 5. Decodifica e riproduzione.

Una volta che i dati video raggiungono gli utenti, i loro dispositivi decodificheranno e decomprimeranno il video segmento per segmento nei dati binari grezzi. E, con un lettore video, l'utente può vedere le informazioni visive e riprodurre il video.

### **Perché usare una CDN per lo *streaming* in diretta?**

Le CDN aiutano a migliorare la qualità del *live streaming* distribuendo il contenuto ai *server* di *streaming* più vicini all'utente finale. In particolare, i fornitori di CDN migliorano lo *streaming* di video *live* nei seguenti modi:

1. Garantiscono una larghezza di banda sufficiente nei periodi di picco del traffico.

Le CDN aiutano a evitare che i *server* di origine vengano sovraccaricati se le richieste superano il limite di larghezza di banda.

Se un *live streaming* vede improvvisamente un rapido aumento delle visualizzazioni e tutti gli utenti richiedono di accedere a contenuti da un singolo *server* di origine, si può creare un collo di bottiglia e provocare tempi di inattività del *server*. Con le CDN, il *server* può essere protetto da questi scenari e la responsabilità della distribuzione del contenuto viene distribuita sulla rete dei *server* di *streaming*.

2. Riducono la latenza e il tempo di andata e ritorno.

Memorizzando il contenuto nella *cache* dei *server* CDN più vicini agli utenti finali, le CDN riducono la necessità che le richieste di *live streaming* arrivino fino al *server* di origine. Ciò riduce il tempo di andata e ritorno o RTT e, soprattutto, riduce al minimo la latenza e il *buffering* per mantenere lo *streaming* in tempo reale.

3. Aiutano lo *streaming* in diretta per un pubblico globale.

Poiché la distribuzione avviene tramite *server* periferici situati in tutto il mondo e posti all'interno di una rete di distribuzione di contenuti, le CDN forniscono scalabilità nel *live streaming* a livello globale. E non solo, indipendentemente da dove si trova l'utente, l'esperienza di visualizzazione è la stessa e la latenza e il *buffering* sono ridotti al minimo tramite i *server* CDN più vicini all'utente finale.

4. Riducono il carico di lavoro sui *server* d'origine.

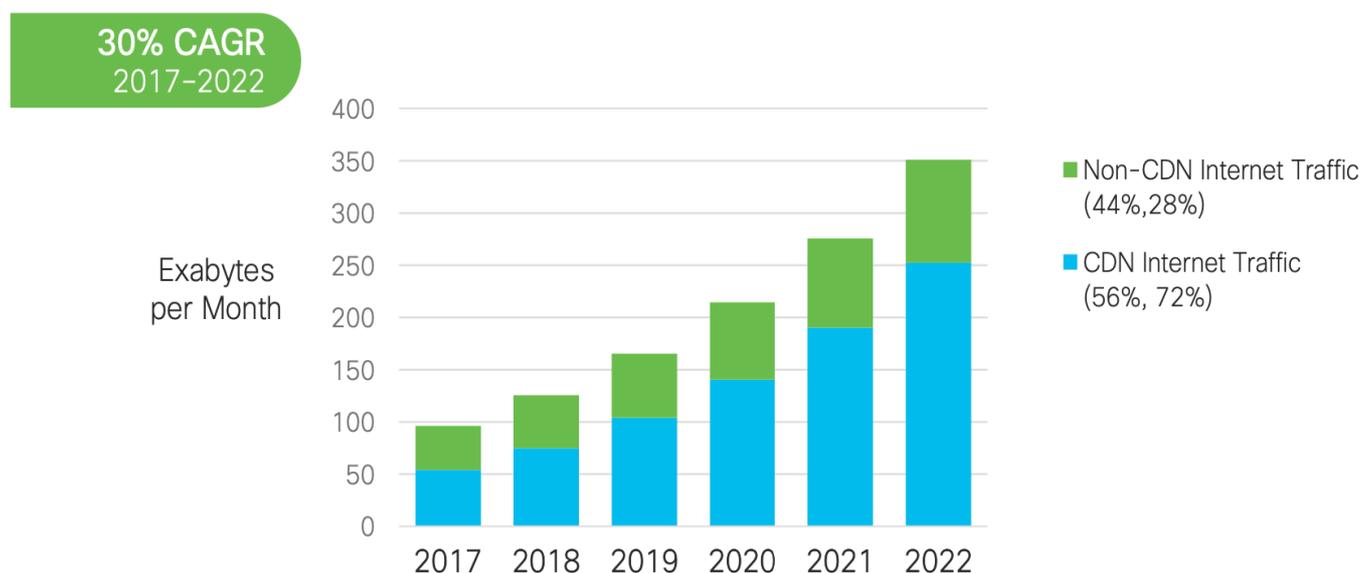
Le CDN aiutano a scaricare gran parte del carico di lavoro dai *server* di origine alla rete. Dal momento che viene richiesta molta potenza di calcolo per rispondere alle richieste, e ancora di più per lo *streaming live*

video, le CDN essenzialmente proteggono i *server* di origine dal sovraccarico e li mantengono operativi. Lo stesso approccio aiuta a proteggere i *server* da attacchi *Denial of Service* o DDoS distribuiti, come esposto in precedenza.

## 2.8 Evoluzione del traffico su CDN

Come già accennato, gran parte del traffico Internet viene gestito tramite CDN. Nello specifico entro il 2022 il 72% del traffico sarà trasportato tramite *Content Delivery Network* (CDN), in aumento rispetto al 56% del 2017 [Grafico 27], facendo aumentare la quota di traffico gestita ai bordi della rete (*Edge computing*)<sup>41</sup>.

Grafico 27 - L'evoluzione del traffico su CDN.



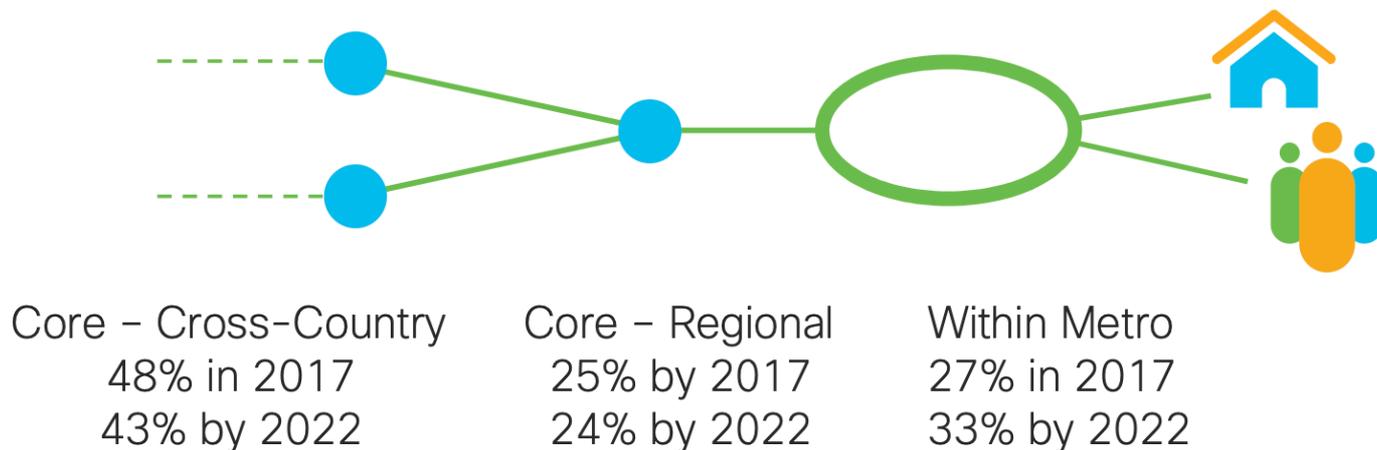
Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

A livello globale, infatti, nel 2022 il 35% del traffico Internet sarà trasportato tramite il paradigma di *edge computing*, segnando una crescita rispetto al 22% del 2016. L'elaborazione ai bordi della rete sarà essenziale, quindi, per garantire latenze dell'ordine di 1 ms, richieste da tutta una serie di servizi innovativi, non solo video, caratterizzanti la *Digital Economy*.

Il cambiamento di Internet in ottica di elaborazione ai bordi della rete è confermato anche dalle previsioni di crescita del traffico nelle reti di area metropolitana e di area regionale, che entro il 2022 gestiranno rispettivamente il 33% e il 24% di tutto il traffico globale [Figura 28].

<sup>41</sup> Cisco annual internet report, 2017-2022, Cisco, 2019.

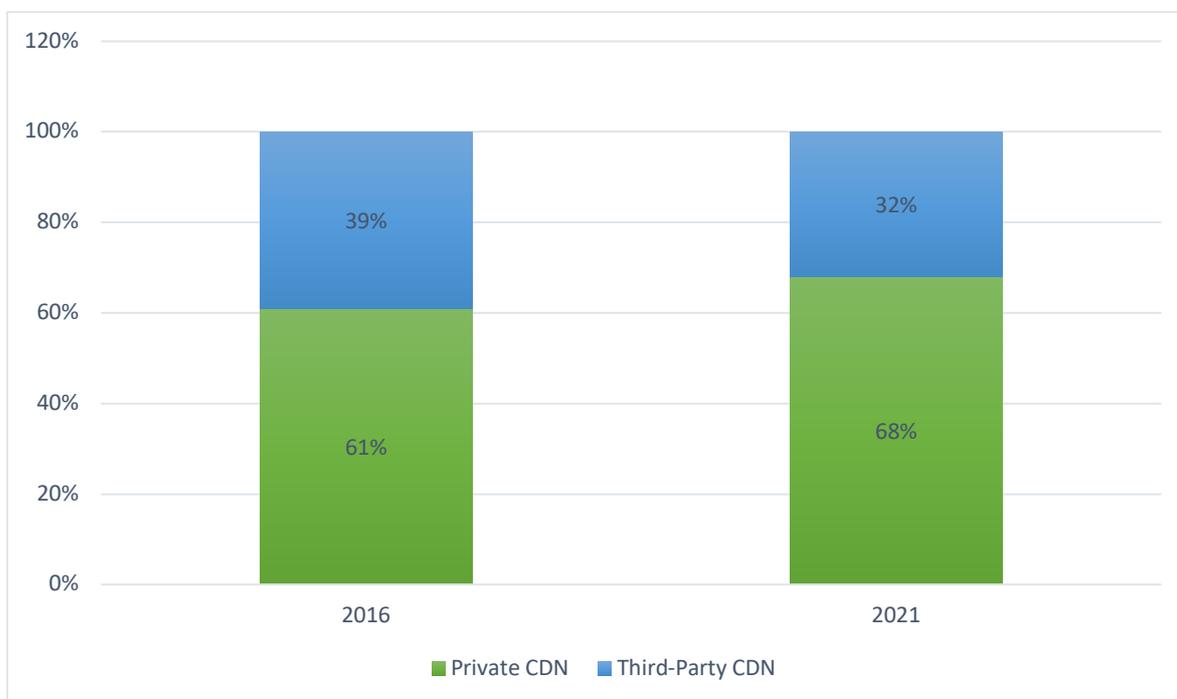
Figura 28 - Spostamento del traffico Internet dal core ai bordi della rete.



Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

Sempre in ambito CDN, già oggi la maggior parte del traffico è trasportata da CDN private ossia CDN realizzate e gestite da *content provider* che le utilizzano per trasmettere i propri contenuti. Esempi di operatori di CDN privati sono Google, Amazon, Facebook e Microsoft. Secondo Cisco, già entro la fine del 2021, circa il 70% del traffico trasportato tramite CDN sarà relativo a CDN private<sup>42</sup> [Grafico 29].

Grafico 29 - Private CDN vs Third-Party CDN.



Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

<sup>42</sup> Cisco Visual Networking Index™ (Cisco VNITM), Cisco.

Inizialmente, con l'avvento delle prime CDN, gli attori che godevano di una CDN di proprietà erano pochi, per questo il mercato era caratterizzato da una forte domanda di un servizio che poteva però essere offerto da pochi, con il conseguente aumento del prezzo. Questa situazione però non era ottimale poiché il soggetto, che pagava una determinata somma per usufruire della CDN non di sua proprietà, non era in grado di assicurare un'adeguata QoE per l'utente, dato che non godeva della *governance* sulla rete. Con la crescita esponenziale del traffico nella rete Internet e con l'avvento dello *streaming* video si è passati da una monofornitura di CDN a multi-CDN, ma anche questo non era sufficiente: si comprese ben presto che l'unica soluzione era la realizzazione di CDN private (vedi l'esempio di Netflix, Amazon, Google).

Secondo Philippe Tripodi, *co-founder* di Mainstreaming, tre sono gli elementi fondamentali per garantire un'elevata QoE per l'utente:

1. *Governance* della rete.

L'uso di *Content Delivery Provider* pone, di solito, limitazioni sia sulla qualità che sui costi. La qualità del servizio offerto è difficile da garantire all'utente perché vi sono importanti limitazioni sui valori conseguibili per i KPIs (*throughput*, *download time*, *video delay*). I costi di *delivery*, invece, tendono ad aumentare in quanto crescono i volumi e la qualità richiesta dai servizi video (4K, 8K, realtà aumentata).

Oggi le *Content Delivery Network* hanno limiti sulle prestazioni, poiché le loro piattaforme di *Content Delivery* spesso sono interconnesse con le reti dei Telco, ma non sono collocate nelle loro reti, in quanto molti operatori (ad es. Vodafone) non lo consentono. Anche nel caso in cui esse siano inserite nel *core* della rete di un Telco con il conseguente miglioramento delle prestazioni, rimane, però, la grande distanza tra piattaforma e *end-user* e, nel caso di accessi UBB, non si possono offrire i servizi 4K che richiedono una velocità effettiva (*Throughput*) di 20-30 Mbit/s. Inoltre, la distribuzione di piattaforme CD *deep into the Telco network* non è semplice da realizzare: è necessario, infatti, distribuire alcune delle funzionalità nel *core* delle reti. Questa trasformazione delle reti dei Telco è costosa e complessa e, quindi, richiederà molti anni.

2. *Hardware* efficiente, in particolare per quanto riguarda i consumi energetici.

Secondo un recente studio del GeSI, Internet consuma ben il 3% dell'energia elettrica mondiale<sup>43</sup>. In particolar modo sono i ripetitori, i *data center* e le strutture a supporto della rete a generare un consumo così elevato, ancora in buona parte proveniente da fonti fossili.

---

<sup>43</sup> SMART 2020: *enabling the low-carbon economy in the information age*, 2020, GeSI.

La Rete è uno strumento diventato indispensabile ed è anche invisibile: per questo gli utilizzatori non sono ben coscienti di tutto il fabbisogno energetico che questa richiede. Come dichiara Mark Radka, direttore del reparto “Energia e Clima” della sezione Ambiente dell’ONU: “Dietro a ciò che vediamo e usiamo quotidianamente vi sono delle infrastrutture che sono necessarie per alimentare le attività *online* e, spesso, non si riesce a collegare l’utilizzo di Internet con l’impatto che questo ha sull’ambiente”. Proprio in virtù di questa consapevolezza, molti colossi IT come Facebook, Google, Apple, negli ultimi anni hanno intrapreso delle iniziative per minimizzare l’impatto ambientale.

3. Un *Software* adeguato, che sia in grado di gestire i picchi nel traffico Internet e che garantisca il percorso più veloce per i pacchetti/contenuti dall’origine all’*end-user*, assicurando la latenza minore.

Proprio per questo circa il 70 % del traffico è gestito da CDN private.

Tra gli aspetti evidenziati da Philippe Tripodi, la *governance* della rete, insieme ad un’infrastruttura adeguata, sono gli elementi centrali per assicurare un’elevata QoE, la continuità del servizio e il controllo dei costi.

# CAPITOLO 3: LA CONTENDIBILITÀ NEL MERCATO ITALIANO

Sia a livello italiano che a livello internazionale il *leader* del settore è Akamai.

Il presente elaborato mira a stabilire se la posizione che Akamai ha raggiunto nel mercato del *content delivery*, dopo 23 anni dalla sua nascita nel 1998, sia contendibile da altri *player*, siano essi *incumbent* o potenziali.

Per condurre questo tipo di analisi, data la scarsità di dati da cui poter attingere, si è proceduto tramite interviste ad alcuni esperti dei principali *player* nel mercato: Stefano Pateri e Luca Moglia (Akamai), Federico D'Alessio e Miriam Ruberto (Amazon Web Services) e Philippe Tripodi (Mainstreaming). Attraverso il confronto con rappresentanti di tali aziende si è potuto comprendere più in profondità le dinamiche competitive caratterizzanti il mercato del *content delivery*, la contendibilità del mercato e i possibili scenari futuri.

## 3.1 Il *leader* del mercato: Akamai overview

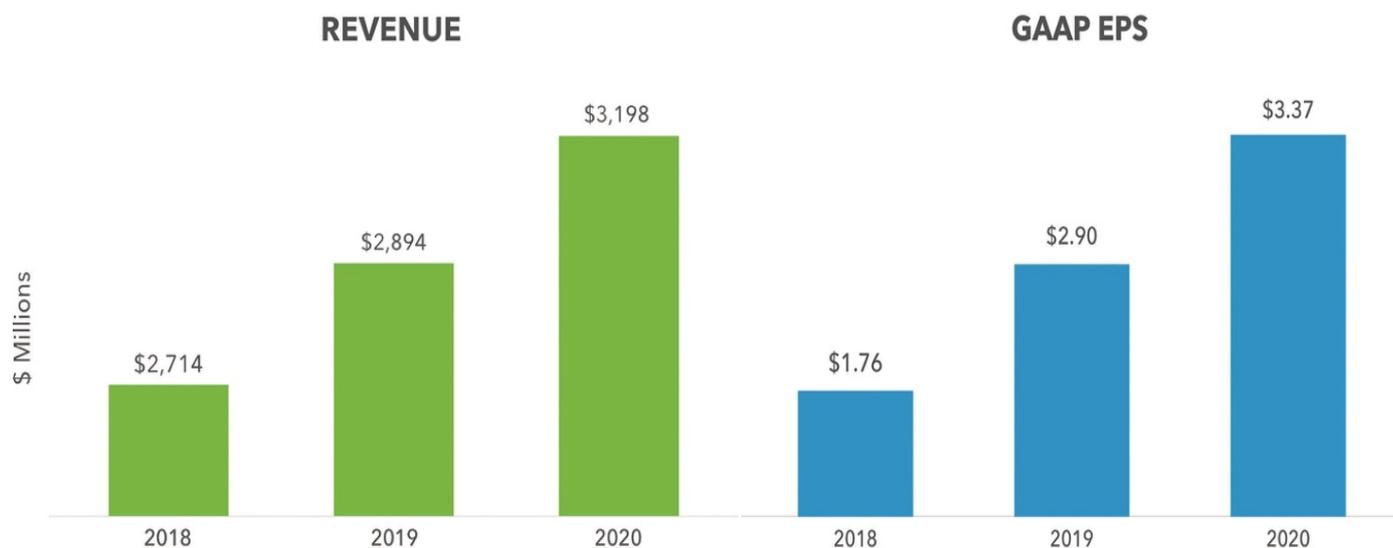
Akamai technologies è stata costituita nel Delaware nel 1998 e ha sede a Cambridge, Massachusetts. La società fornisce soluzioni per la protezione, la distribuzione e l'ottimizzazione di contenuti e applicazioni aziendali su Internet. La piattaforma di Akamai, in continua crescita e sviluppo, rappresenta il valore aggiunto e il vero vantaggio competitivo rispetto ai *competitor*. Nel corso degli anni Akamai ha consolidato i rapporti di *peering* e ha raggiunto livelli di penetrazione con gli ISP difficilmente raggiungibili. Nessun *provider* ad oggi (Amazon, Google, Netflix, Facebook) ha la stessa struttura. Akamai da 23 anni sviluppa il proprio portfolio, garantendo scalabilità, *performance* e sicurezza elevata.

Nel 2020 ha fatto registrare un fatturato di circa 3,2 miliardi di dollari e nessun *player* nel mercato ha numeri di questa portata. Da un punto di vista finanziario, Akamai ha aumentato le entrate in ciascuno degli ultimi tre anni fiscali e nello stesso periodo ha fatto registrare una redditività positiva. Il grafico 30 mostra il fatturato e gli utili per azione, calcolati in conformità con i principi contabili accettati negli Stati Uniti, o GAAP, per gli ultimi tre anni fiscali<sup>44</sup>.

---

<sup>44</sup> Akamai Annual Report 2020, Akamai, 2020.

Grafico 30 - Fatturato e utile per azione di Akamai negli ultimi tre anni fiscali.



Fonte: Akamai Annual Report 2020, Akamai, 2020

Dal 2010 ad oggi sono nate aziende che cercano di proporre un'offerta simile ad Akamai, adottando una strategia molto aggressiva sul prezzo. La *mission* di Akamai, però, è garantire un'*experience* e una *performance* di qualità ed elevati *standard* di sicurezza per i clienti e non ha l'obiettivo di competere sul prezzo.

La piattaforma *core business* è l'*Akamai Intelligent Edge Platform*, progettata per aiutare i clienti a sfruttare la potenza e la portata di Internet proteggendoli al contempo da minacce dannose per la loro attività.

Tale piattaforma è distribuita a livello globale e comprende:

- 325.000 *server* in più di 130 paesi.
- Una rete composta da 1700 *network*.
- Una relazione solida con vari operatori telefonici, che permette ad Akamai di posizionare i propri *server* all'interno dei vari POP dei Telco.

Akamai distribuisce *server* e tecnologia alla periferia della rete, stabilendo punti di contatto lungo il suo perimetro. Questo approccio offre informazioni uniche su volumi di traffico, congestione, schemi di attacco, vulnerabilità e altre attività nel complesso di reti e sistemi *cloud*. Akamai propone, quindi, ai propri clienti soluzioni ad *hoc* per garantire sicurezza e protezione da minacce ed attacchi, consentendo loro di svolgere in modo sicuro la loro attività mentre interagiscono e si intrattengono con i loro rispettivi clienti.

### 3.1.1 La strategia di Akamai

La pandemia COVID-19, causa di sconvolgimenti globali nell'ultimo anno, ha rafforzato la convinzione del ruolo vitale di Internet nel trasformare le modalità con cui si scambiano idee e informazioni, si conducono gli affari e si affronta la vita di tutti i giorni. In tutto il mondo c'è stato un passaggio al lavoro a distanza, che deve essere svolto in modo sicuro e affidabile. Il consumo di *media* su Internet (film, programmi TV e giochi) è aumentato drasticamente. Allo stesso tempo, le minacce alla sicurezza hanno continuato a diventare sempre più frequenti e avanzate<sup>45</sup>. Questa tendenza non è nuova, ma è stata accelerata dalla crisi sanitaria globale e Internet svolgerà un ruolo sempre più importante nella vita di ciascuno.

La strategia di Akamai è quella di soddisfare le esigenze di questa trasformazione offrendo soluzioni di sicurezza, prestazioni e consegna che diano ai clienti il vantaggio competitivo di cui hanno bisogno. L'*Akamai Intelligent Edge Platform* è fondamentale, si posiziona ai margini di Internet da oltre 20 anni ed è distribuita in circa 4.100 sedi, insieme a *software* e algoritmi sofisticati. Attraverso questa presenza unica e pervasiva all'*edge*, si avvicinano le applicazioni, le esperienze e le decisioni aziendali agli utenti con l'obiettivo di tenere lontani attacchi e minacce.

Più specificamente, le caratteristiche chiave della piattaforma includono le capacità di:

- Identificare, assorbire e bloccare le minacce alla sicurezza.
- Instradare in modo efficiente il traffico, lontano dai punti problematici di Internet.
- Aiutare i clienti a implementare un modello di sicurezza zero *trust* come descritto di seguito.
- Rilevare quali dispositivi utilizzano gli individui e ottimizzare la consegna dei contenuti.
- Proteggere e gestire l'identità del cliente.
- Fornire ai clienti informazioni commerciali, tecniche e analitiche sulle loro operazioni *online*.
- Comprendere i diversi tipi di traffico dei siti *web* in modo che i clienti possano rispondervi.

La scala raggiunta da Akamai, la tecnologia unica, la forza lavoro altamente qualificata, i livelli di sicurezza, le solide relazioni con migliaia di marchi importanti e l'attenzione incessante e personalizzata alle esigenze di clienti e *partner* creano un valore significativo per gli azionisti, forniscono un vantaggio rispetto ai concorrenti e pongono l'azienda in una posizione dominante per il futuro.

---

<sup>45</sup> *Il 2021 sarà un anno d'oro per lo streaming live. Ma anche per il cybercrime*, 18 gennaio 2021.

### 3.1.2 La tecnologia e il *network*

L'Akamai *Intelligent Edge Platform* fornisce le basi tecnologiche per tutti i servizi e le soluzioni offerte da Akamai. Utilizza i dati generati in relazione a ciascuna delle soluzioni per migliorare e aumentare la funzionalità della rete *overlay* e garantire un'elevata efficacia dei vari servizi offerti. L'Akamai *Intelligent Edge Platform* sfrutta più di 325.000 *server* distribuiti in più di 1.400 reti che vanno dai grandi *provider* di reti dorsali, ai *provider* di servizi Internet di medie e piccole dimensioni (ISP), ai *provider* di *modem* via cavo e satellitari, alle università e ad altre reti.

Distribuendo *server* all'interno di un'ampia varietà di reti in più di 130 paesi, Akamai è in grado di gestire e controllare meglio il *routing* e la qualità della consegna a utenti geograficamente distanti. Akamai gode anche di migliaia di relazioni di *peering* che forniscono percorsi diretti alle reti degli utenti finali, che riducono la perdita di dati, fornendo anche potenzialmente più opzioni per la consegna a costi ridotti. Per rendere efficace questa distribuzione di vasta portata, vengono utilizzate tecnologie specifiche come il *routing* avanzato, il bilanciamento del carico, la raccolta e il monitoraggio dei dati.

Il *software* di *routing* intelligente è progettato per garantire ai visitatori del sito *web* un caricamento rapido delle pagine, l'accesso alle applicazioni e l'assemblaggio dei contenuti ovunque si trovino su Internet e indipendentemente dalle condizioni del traffico globale o locale. Un *team* di professionisti dedicati sono inseriti all'interno di un centro di comando delle operazioni di rete 24 ore al giorno, sette giorni alla settimana, per monitorare e reagire ai modelli e alle tendenze del traffico Internet. Vengono, inoltre, distribuiti frequentemente miglioramenti del *software* a livello globale per rafforzare e migliorare l'efficacia della rete. La piattaforma offre anche flessibilità: i clienti possono modificare in maniera dinamica l'utilizzo della tecnologia di Akamai grazie alla possibilità di scalare su richiesta in base alla rete di cui hanno bisogno, per supportare un traffico molto variabile e una rapida crescita, senza la necessità di un'infrastruttura interna costosa e complessa.

### 3.1.3 I principali servizi offerti

#### **Cloud e sicurezza**

Le soluzioni di sicurezza aziendale e *cloud* di Akamai sono progettate per proteggere l'infrastruttura, i siti *web*, le applicazioni, le interfacce di programmazione delle applicazioni (API) e gli utenti da molteplici attacchi informatici e minacce *online*, migliorando al contempo le prestazioni. I servizi forniscono protezioni personalizzabili per le organizzazioni che cercano un maggiore controllo sulla sicurezza del *web* e delle applicazioni, nonché soluzioni di facile implementazione per le organizzazioni senza una solida esperienza. Vengono inoltre offerti *framework* e strumenti per abilitare nuovi modelli per l'accesso aziendale da remoto in modo tale da sostituire il tradizionale approccio di rete privata virtuale (VPN) e facilitare la connessione

sicura di utenti e dispositivi a Internet; in particolare, viene abilitato un approccio *zero trust* alla sicurezza della rete che specifica, applicazione per applicazione, quali utenti e dispositivi possono accedere ad applicazioni e a dati. Con *zero trust* le aziende possono identificare, bloccare e mitigare in modo proattivo le minacce, inclusi *malware*, *ransomware* e attacchi di *phishing*.

Ulteriori funzionalità di sicurezza di Akamai includono sicurezza API, mitigazione dell'abuso di credenziali, protezione contro DDoS, gestione delle identità, protezione dalle minacce nel *browser*, *firewall* per applicazioni *web* e *gateway web* sicuro. Akamai intende concentrare gran parte dei suoi investimenti attuali e futuri nell'innovazione di soluzioni di sicurezza, per determinare un'opportunità di crescita dei ricavi. In particolare, l'attività di sicurezza è cresciuta rapidamente negli ultimi anni, come mostrato nel grafico 31.

Grafico 31 - Ricavi di Akamai provenienti dalla sicurezza.



Fonte: Akamai Annual Report 2020, Akamai, 2020

### **Prestazioni *web* e *mobile***

Le soluzioni offerte da Akamai per le prestazioni *web* e *mobile* sono progettate per consentire a siti *web* dinamici e alle applicazioni di avere tempi di risposta rapidi, indipendentemente da dove si trova l'utente e da quale dispositivo e *browser* stia utilizzando per connettersi ad Internet. Questi servizi sfruttano l'ottimizzazione intelligente delle prestazioni, il monitoraggio in tempo reale, l'*offload* dell'origine, l'affidabilità della rete e informazioni dettagliate che consentono alle aziende di identificare e affrontare i problemi relativi alle prestazioni. Le funzionalità di Akamai per le prestazioni *web* e *mobile* includono anche la gestione del traffico globale, l'accelerazione del sito, il bilanciamento del carico delle applicazioni, l'ottimizzazione automatica di immagini e video, test del carico su larga scala e monitoraggio degli utenti reali.

## ***Media delivery***

Le soluzioni di *media delivery* di Akamai sono progettate per consentire alle aziende di attuare le proprie strategie di distribuzione dei *media* digitali affrontando i requisiti di volume e portata globale, migliorando l'esperienza dell'utente finale, aumentando l'affidabilità e riducendo i costi dell'infrastruttura di Internet. Alla base di queste soluzioni c'è una tecnologia in grado di affrontare velocità di connessione variabili, differenti tipologie di dispositivi, di facilitare l'accesso da diverse posizioni in tutto il mondo, di accelerare il *download* di *file* di grandi dimensioni, di fornire in modo affidabile contenuti *live* di alta qualità su vari dispositivi e piattaforme, di consentire la visione di video *online* in tempo reale e di offrire archiviazione *cloud* distribuita a livello globale progettata per la resilienza, l'elevata disponibilità e l'ottimizzazione delle prestazioni in tempo reale. Le soluzioni di distribuzione multimediale di Akamai includono *streaming* video e servizi di riproduzione video, distribuzione di giochi e *software*, operazioni di trasmissione, sistema di nomi di dominio autorevole o DNS, risoluzione, dati e analisi.

## ***Edge Computing***

Le funzionalità di *edge computing* sono progettate per consentire agli sviluppatori di distribuire il codice a livello di *edge* della rete. Questo approccio avvicina i dati e il processo decisionale agli utenti e ai sistemi che agiscono su di essi, in modo che i gruppi di lavoro possano intervenire rapidamente sulle capacità esistenti per soddisfare le mutevoli esigenze dei clienti e creare soluzioni a bassa latenza che forniscano esperienze rapide, reattive e personalizzate. Con l'accesso all'*Akamai Intelligent Edge Platform*, le aziende e gli sviluppatori ottengono un'implementazione rapida e una scala globale senza gestire alcuna infrastruttura interna aggiuntiva.

## ***Carrier***

Le offerte di *carrier* di Akamai sono progettate per aiutare i clienti a gestire una rete efficiente in termini di costi, che capitalizza sulla crescita del traffico, sui nuovi servizi di sicurezza per gli abbonati, sulla gestione del traffico e la distribuzione dei contenuti. Le soluzioni aiutano gli operatori a vendere offerte di protezione dalle minacce informatiche facili da implementare per i loro abbonati. Le offerte includono protezione da *phishing*, virus, *malware* e *ransomware*. Inoltre, i servizi di sicurezza dell'operatore includono il controllo genitori per personalizzare l'accesso a Internet. Vengono offerti anche un'infrastruttura DNS e soluzioni di distribuzione dei contenuti per i vettori attraverso l'offerta DNS intelligente.

## **Servizi e supporto**

Akamai è in grado di offrire una serie di servizi e un supporto progettati per assistere i clienti nell'integrazione, configurazione, ottimizzazione e gestione delle offerte. Una volta inseriti sulla piattaforma *Akamai Intelligent Edge Platform*, i clienti possono fare affidamento su servizi professionali e su esperti di sicurezza per soluzioni personalizzate, risoluzione dei problemi e assistenza clienti 24 ore su 24, 7 giorni su 7. Ulteriori funzionalità

sono disponibili per le aziende che acquistano soluzioni di sicurezza *premium*, tra cui un *team* di *account* tecnico dedicato, monitoraggio del servizio proattivo, gestione del supporto tecnico personalizzato, monitoraggio del traffico di sicurezza, revisioni tecniche della sicurezza e avvisi sulle minacce.

### 3.1.4 Focus sulla CDN di Akamai

Akamai ha creato e controlla tuttora la CDN più distribuita al mondo e gestisce oltre il 30% del traffico Internet. Forte del portafoglio di servizi più ampio del settore, Akamai fornisce soluzioni CDN di ultima generazione a tutti gli operatori.

Akamai Aura Licensed CDN è una *suite* di *software* per operatori di CDN che rende possibile la distribuzione di servizi video IP su qualsiasi dispositivo. Aura Managed CDN è una soluzione di *hosting* CDN che fornisce una rete per la distribuzione dei contenuti chiavi in mano e altamente scalabile, fondata su un'infrastruttura gestita da Akamai. I servizi *media delivery* di Akamai rispondono alle richieste del pubblico per quanto riguarda lo *streaming* di contenuti e il *download* di grandi *file on-demand*.

Le funzionalità e le soluzioni CDN di Akamai sono studiate per far fronte alle principali sfide relative alle reti di ultima generazione, grazie a:

- Funzioni avanzate per l'ottimizzazione delle prestazioni *web*, che agiscono sulle prestazioni *mobile*, *web* e CDN per migliorare la *user experience*, le conversioni e, in ultima analisi, il fatturato.
- Soluzioni di distribuzione dei video di elevata qualità, pronte a gestire facilmente il *boom* dei video *online* e le esigenze degli utenti in termini di valore e rapidità di accesso.
- Soluzioni per la sicurezza delle CDN e del *cloud*, finalizzate alla difesa di siti *web*, applicazioni *web* e infrastrutture, senza intaccare le prestazioni dei siti o delle applicazioni in questione.
- Soluzioni di *compliance* che assicurano la piena conformità alle normative vigenti, come i requisiti Health Insurance Portability and Accountability Act (HIPAA) e Payment Card Industry (PCI).
- Un *Tool* per l'accelerazione della distribuzione delle applicazioni, sviluppato per offrire agli utenti di tutto il mondo le applicazioni aziendali alla velocità che si aspettano.
- Un'architettura altamente distribuita, che colloca il *server* Akamai a una sola rete di distanza dall'85% degli utenti internet.
- Soluzioni orientate all'usabilità, che semplificano le interazioni tecniche e ampliano le opzioni *self-service* per i servizi CDN di prossima generazione.

### 3.1.5 L'ambiente competitivo

Il mercato in cui Akamai opera è estremamente competitivo e caratterizzato da tecnologie in rapido sviluppo, da *standard* di settore in evoluzione e da frequenti innovazioni di prodotti e servizi. Si prevede che la concorrenza sui servizi offerti da Akamai aumenterà sia da parte di imprese *incumbent* sia da parte di nuovi entranti nel mercato. La competizione tra i vari *player* si basa principalmente su:

- Prestazioni e affidabilità delle soluzioni e dei servizi offerti.
- Ritorno sull'investimento in termini di risparmio sui costi e nuove opportunità di guadagno per i clienti.
- Ridotta complessità dell'infrastruttura.
- Raffinatezza e funzionalità delle offerte.
- Scalabilità.
- Sicurezza.
- Facilità di implementazione e fruizione del servizio.
- Servizio Clienti.
- Prezzo.

Akamai si trova in concorrenza con aziende che offrono prodotti e servizi che mirano a garantire elevate prestazioni Internet, con aziende che forniscono servizi di *hosting*, servizi di distribuzione di contenuti Internet, soluzioni di sicurezza, soluzioni tecnologiche utilizzate dai vettori per migliorare l'efficienza dei loro sistemi, servizi di distribuzione di contenuti in *streaming* e soluzioni basate sull'utilizzo di apparecchiature volte a risolvere i problemi relativi alle prestazioni di Internet, come bilanciatori del carico e *switch* del *server*.

Altre società offrono la distribuzione *online* di risorse multimediali digitali attraverso modelli di fatturazione basati sulla pubblicità o di compartecipazione alle entrate che possono rappresentare un metodo alternativo per addebitare la consegna di contenuti e applicazioni su Internet.

Inoltre, i clienti esistenti e potenziali possono decidere di acquistare o sviluppare il proprio *hardware*, *software* o altre soluzioni tecnologiche piuttosto che affidarsi a un fornitore di terze parti come Akamai. I servizi di sicurezza offerti da Akamai competono con le varie soluzioni fornite da fornitori di *hardware* e *software*, molti dei quali più affermati di Akamai.

### 3.1.6 I principali rischi

Il tasso di crescita dei ricavi di cui Akamai ha goduto negli ultimi anni potrebbe non proseguire e addirittura comprimersi, il che avrebbe un impatto negativo sulla redditività e sul prezzo delle azioni.

Le entrate dipendono dalla quantità di traffico che viene fornito, dalla continua crescita della domanda per le prestazioni e soluzioni di sicurezza offerte e dalla capacità di mantenere i prezzi che vengono applicati ai vari clienti. Nel 2020 Akamai ha fatto registrare un aumento significativo delle entrate derivanti dalle soluzioni multimediali, in gran parte dovuto al maggiore consumo di *media*, di giochi *online* e di ordini casalinghi durante la pandemia di COVID-19. Numerosi altri fattori influiscono sulla crescita del traffico:

- Il ritmo di introduzione di iniziative di distribuzione video *over-the-top* (OTT) da parte dei clienti.
- La popolarità delle offerte di *streaming* dei clienti rispetto alle offerte da parte di aziende che non utilizzano le soluzioni offerte da Akamai.
- La variazione positiva della popolarità del *gaming online*.
- I *media* e altri clienti che utilizzano i propri *data center* e implementano approcci di consegna che limitano o eliminano la dipendenza da fornitori di terze parti come Akamai.
- Le condizioni macroeconomiche generali e le pressioni nel settore.

I livelli di traffico sulla rete hanno iniziato a stabilizzarsi nel quarto trimestre del 2020. Di conseguenza non si prevede che la crescita del traffico nel 2021 continuerà agli stessi livelli che sono stati registrati all'inizio del 2020, in assenza di altri sviluppi significativi del settore.

Negli ultimi anni le aziende che offrono soluzioni di sicurezza hanno fatto registrare una crescita significativa dei ricavi. Per mantenere o accelerare la crescita dei ricavi provenienti dalla sicurezza è necessario aumentare la posizione dominante di Akamai in tale ambito e sviluppare nuove soluzioni in un ambiente in cui le minacce alla sicurezza sono in continua evoluzione. L'azienda ha necessità di garantire che i propri servizi funzionino in modo efficace e che siano competitivi con i prodotti offerti da altri.

Akamai ha fatto registrare un calo dei ricavi negli ultimi trimestri relativo alle soluzioni per le prestazioni *web* e si prevede che questa tendenza continui a causa della crescente pressione sui prezzi in alcune aree geografiche, determinata dalla concorrenza e delle condizioni commerciali che interessano molti dei clienti di Akamai, nello specifico in riferimento a settori come i viaggi e l'ospitalità. Nel 2020, molti di questi clienti hanno dovuto affrontare interruzioni significative della propria attività a causa dell'emergenza sanitaria pubblica internazionale associata alla pandemia di COVID-19.

Le ricadute economiche della pandemia sono proseguite nel 2021 e si prevede possano avere conseguenze di vasta portata in molti settori, tra cui fallimenti, riduzioni della spesa tecnologica e recessione economica. Ognuna di queste circostanze avrebbe un impatto negativo sui ricavi.

La capacità da parte di Akamai di aumentare le proprie entrate complessive dipende anche da molti altri fattori, come ad esempio:

- Fidelizzazione dei clienti esistenti, mantenendo i servizi attuali e offrendo loro nuove soluzioni.
- Sviluppare e vendere nuove soluzioni innovative e accattivanti.
- Affrontare la potenziale mercificazione delle soluzioni basate sulla consegna, che può portare a prezzi più bassi e alla perdita di clienti a favore dei concorrenti.
- Contrastare le *policy multivendor* che potrebbero indurre i clienti a ridurre la loro dipendenza da Akamai.
- Adattarsi ai cambiamenti nei modelli di contratto con i clienti, da una struttura di ricavi *committed* (fissa/stabilita) a un approccio "*pay-as-you-go*".
- Gestire l'impatto dei cambiamenti nelle condizioni economiche generali.

Se Akamai non sarà in grado di aumentare i ricavi, la sua redditività e il prezzo delle azioni potranno risentirne.

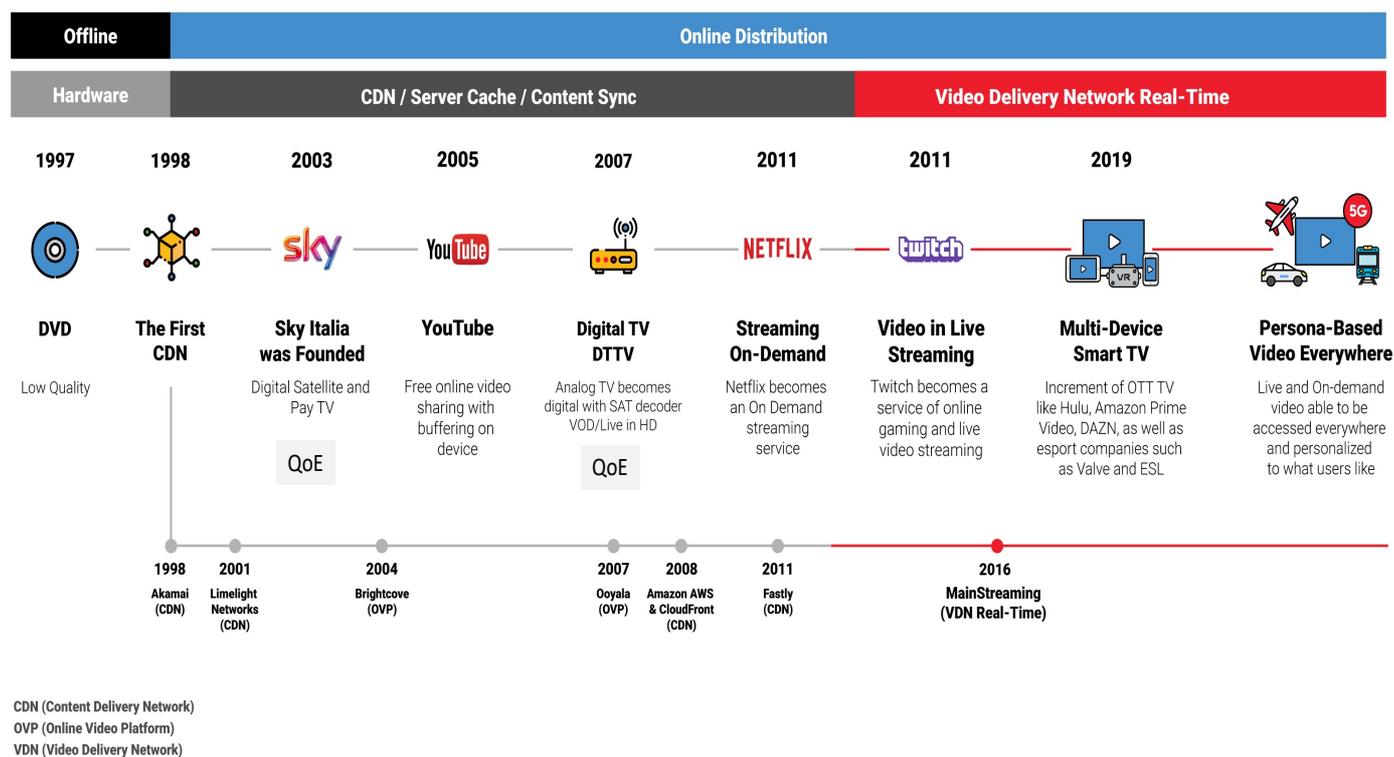
*Figura 32 - Bilancio degli ultimi 5 esercizi di Akamai.*

Year ended December 31,	2020	2019	2018	2017	2016
Revenue	\$ 3,198,149	\$ 2,893,617	\$ 2,714,474	\$ 2,489,035	\$ 2,347,988
Total costs and operating expenses	2,539,615	2,344,699	2,351,975	2,174,746	1,881,478
Income from operations	658,534	548,918	362,499	314,289	466,510
Net income	557,054	478,035	298,373	222,766	320,727
Basic net income per share	3.43	2.94	1.78	1.30	1.83
Diluted net income per share	3.37	2.90	1.76	1.29	1.82
Cash, cash equivalents and marketable securities	2,496,875	2,372,378	2,101,171	1,279,528	1,616,329
Total assets	7,764,130	7,006,886	5,461,770	4,648,916	4,432,190
Convertible senior notes – due 2019	—	—	686,552	662,913	640,087
Convertible senior notes – due 2025	953,066	912,719	874,080	—	—
Convertible senior notes – due 2027	953,641	927,072	—	—	—
Long-term operating lease liabilities	715,404	692,181			
Other long-term liabilities	132,553	123,620	185,121	166,840	156,329
Total stockholders' equity	4,251,296	3,657,958	3,191,860	3,362,469	3,270,218

*Fonte: Akamai Annual Report 2020, Akamai, 2020*

## 3.2 I competitors: lo scenario di riferimento

Figura 33 - L'evoluzione del video e principali attori nel mercato.



Devono essere distinti tre diversi livelli di *competition* nel mercato delle CDN:

### 1. Operatori *Big tech*

Akamai ha raggiunto un rapporto 1:100 rispetto alle cosiddette aziende-stato, come Facebook, Amazon, Apple, Google, Netflix. Si possono distinguere gli operatori *big tech* verticali come Netflix, che detiene le proprie infrastrutture e a seconda delle occasioni prende in prestito dei pezzi di rete da altri operatori. I *player* invece più differenziati come Amazon e Google sono caratterizzati da un *core business* e da una serie di adiacenze.

Per quanto riguarda Amazon, i servizi informatici in *cloud* (ossia il *core business* di AWS) hanno ormai assunto un'importanza maggiore rispetto all'*e-commerce*, infatti pesano più della metà rispetto a quest'ultimo in termini di utili. Nel campo dei servizi informatici l'obiettivo principale di Amazon è quello di andare ad acquisire la professionalità degli sviluppatori dei codici e delle applicazioni, così da riuscire a trasformare i loro *software* e renderli facilmente integrabili con le piattaforme di Amazon stesso: è in tale contesto che il colosso americano compete maggiormente. Amazon potrebbe ritenere strategico ampliare e sviluppare la propria infrastruttura di *content delivery* per garantire una QoE elevata agli utenti per il *live streaming* di Amazon Prime, dato che sta investendo ingenti somme nel mondo dei diritti sportivi (Premier League, Champions League).

Solitamente, grazie ai loro volumi, realtà come Amazon entrano nei mercati obiettivo in perdita e li prosciugano di risorse fissando dei prezzi ad una soglia molto bassa, riuscendo così a svuotare il mercato e a operare in un'ottica di lungo periodo.

Un discorso simile può essere fatto per Google, anche se i servizi aziendali informatici di Google Cloud hanno ancora un peso ridotto rispetto al *business* dei ricavi pubblicitari (*core business*). Infatti, i ricavi pubblicitari rappresentano circa il 90% dei ricavi totali (166 miliardi sui 182,5 totali), mentre i ricavi di Google Cloud nel 2020 ammontavano a 13,1 miliardi di dollari, in aumento (+47%) rispetto agli 8,9 miliardi di dollari del 2019 (e 5,8 miliardi nel 2018), ma questo *business* risulta ancora in perdita operativa per 5,6 miliardi di dollari, evidenziando come sia ancora in modalità di investimento.

Per Akamai e più in generale per gli operatori che offrono servizi di CDN, i *big tech* sono dei *competitor*, ma non rappresentano in questo momento una minaccia poiché per loro la componente di *delivery* non è strategica. La *delivery* ha un'incidenza ridotta rispetto all'impatto che loro puntano ad avere con i loro *core services*. Attualmente quindi, l'obiettivo principale di Amazon, è quello di colpire *player* come IBM e non Akamai, anche perché quando Amazon organizza *convention* a livello mondiale su piattaforma video prende in affitto i servizi di Akamai. (Amazon prime usa Akamai, Apple usa Akamai).

La politica di Amazon è volta a garantire la massima soddisfazione del cliente: in base ai bisogni e alle necessità dei clienti, AWS si muove nel mercato e fa investimenti. Questa strategia può essere percorsa data la grande forza finanziaria di Amazon che usa economie di scala e trasferisce i risparmi al cliente.

Akamai, invece, attualmente si sta concentrando sull'utilizzo di un *network* distribuito all'*edge* che rappresenta il suo principale *asset* strategico (Akamai *Intelligent Edge Platform*), grazie ad accordi e convenzioni con la gran parte degli operatori telefonici nel mondo. La strategia di Akamai è quella di far leva su tale *asset* per rispondere alle esigenze riguardanti la sicurezza (obiettivo *core* per Akamai).

Tabella 34 - Confronto dei fondamentali tra Akamai, AWS e Google Cloud.

AZIENDA	ANNO DI NASCITA	FATTURATO (\$)	UTILE (\$)	DIVIDENDO PER AZIONE <sup>46</sup>
AKAMAI	1998	3,27 MILIARDI	557 MILIONI	0
AWS	2006	45,3 MILIARDI	13,53 MILIARDI	0
GOOGLE CLOUD	2008	13,1 MILIARDI	-5,8 MILIARDI	0

<sup>46</sup> Nessuna delle tre aziende prese in analisi paga dividendi, nonostante realtà come la divisione AWS di Amazon presenti un utile rilevante. Tale scelta è da ricondurre alla natura stessa del settore *tech*, infatti tale comparto non è mai stato famoso per dividendi e cedole. Se le azioni del settore *tech* sono molto restie a staccare dividendi è perché le società a monte di tali azioni sanno perfettamente che per restare competitivi in questo comparto è necessario spendere tantissimo in ricerca e innovazione. Sono gli investimenti il primo pensiero di Amazon, Akamai e Google, non il dividendo.

## 2. Operatori telefonici in forma privata e in forma condivisa e gli operatori di transiti

L'infrastruttura detenuta dagli operatori telefonici è un elemento di differenziazione e vantaggio competitivo. I Telco rappresentano, quindi, un potenziale *competitor*, ma sono maggiori i benefici di una collaborazione tra operatori di *Content Delivery* e Telco rispetto ad una *competition* tra le parti. Questo perché gli operatori di CDN raccordano grazie ai loro *software* i vari *edge* della rete e tale operazione risulta impossibile per gli operatori telefonici: difficilmente vi possono essere condivisioni di POP tra diversi operatori. I Telco vengono visti sia da Akamai che da AWS come dei clienti e in alcuni casi come dei *partner* con cui operare in simbiosi.

## 3. Operatori che si concentrano solo sulla *delivery*

Si tratta di operatori specializzati nel mercato delle CDN, ivi compresi le *startup*. In tale livello di *competition* è importante tenere conto delle date di avvio delle varie imprese. Consideriamo ad esempio Fastly e Limelight, aziende molto aggressive sull'offerta di *delivery* di contenuti, che tuttavia non hanno avuto il tempo e non hanno sostenuto gli investimenti necessari per costruire infrastrutture in grado di competere con Akamai.

Per ordine di *market share*, anche se si parla di un ordine di grandezza dieci volte inferiore ad Akamai, i principali *competitor* di Akamai sono: Limelight, Fastly, Cloudflare e Mainstreaming.

Tabella 35 - Confronto dei fondamentali tra operatori specializzati nelle CDN.

AZIENDA	ANNO DI NASCITA	FATTURATO (\$)	UTILE (\$)	DIVIDENDO PER AZIONE
AKAMAI	1998	3,27 MILIARDI	557 MILIONI	0
LIMELIGHT	2001	230 MILIONI	-19,3 MILIONI	0
FASTLY	2011	291 MILIONI	-95,9 MILIONI	0
CLOUDFLARE	2009	431 MILIONI	-100 MILIONI	0
MAINSTREAMING	2016	1,5 MILIONI	-2 MILIONI	0

Dall'analisi dei fondamentali [Tabella 35], al 31 dicembre 2020, emerge che solo Akamai riesce a generare utili, mentre tutte le altre aziende non sono ancora in una fase avanzata di maturità del *business*. Nello specifico, Limelight, Fastly e Cloudflare stanno sostenendo elevati investimenti che non sono ancora in grado di generare un ritorno positivo mentre Mainstreaming si trova ancora in fase di avvio/crescita.

La scelta di Akamai di non distribuire dividendi nonostante un utile molto elevato deriva da una precisa linea di *policy* interna: *“We have never paid or declared any cash dividends on shares of our common stock or other securities and do not anticipate paying or declaring any cash dividends in the foreseeable future. We currently intend to retain all future earnings, if any, for use in the operation of our business.”*<sup>47</sup>

---

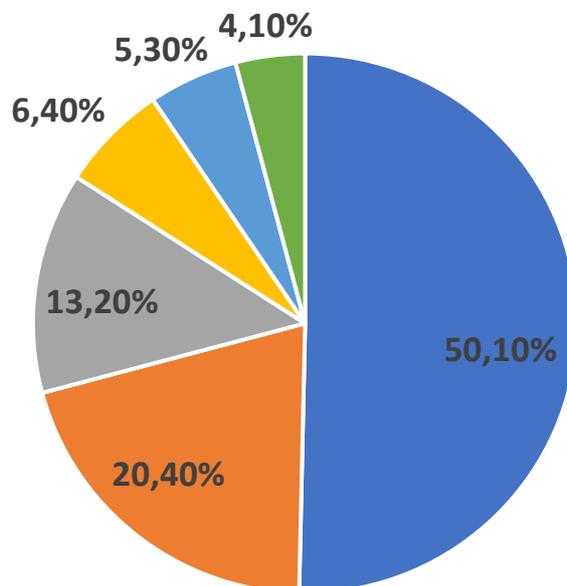
<sup>47</sup> Akamai Proxy Statement 2020, Akamai 2020.

### 3.2.1 Amazon: fatturato e ricavi

Fondata con il nome di Cadabra.com da Jeff Bezos il 5 luglio 1994 e lanciata nel 1995, Amazon.com inizialmente si limitava ad offrire una libreria *online*, ma fin da subito ha allargato la gamma dei prodotti venduti a DVD, CD musicali, *software*, videogiochi, prodotti elettronici, fumetti, abbigliamento, mobilia, cibo, giocattoli e altro ancora per diversificare le sue attività.

Amazon ha chiuso il 2020 con un fatturato di circa 386 miliardi di dollari, in crescita del 38% sul 2019, di cui 216 miliardi dalle vendite di prodotti e 170 miliardi dai servizi. I ricavi registrati, invece, ammontano a 393 miliardi di dollari. Di questi il 50,1% viene dai negozi *online*, con vendite per 197 miliardi di dollari, che spinti dalla pandemia sono aumentati del 46%. La seconda maggiore fonte di ricavi sono i servizi a venditori terzi, soprattutto intermediazione, che hanno portato 80 miliardi di dollari alla società (+57%), il 20% del totale. Amazon Web Services, pur portando la maggior parte dei margini effettivi, genera ricavi per 52 miliardi (+28%), ovvero il 13%. Il resto dei ricavi viene dalle vendite in negozi fisici, con 16 miliardi di dollari (+8%), dagli abbonamenti come Amazon Prime, con 25 miliardi (+35%), e da altre varie attività minori, con 21 miliardi (+66%)<sup>48</sup> [Grafico 36].

Grafico 36 - Suddivisione dei ricavi di Amazon per divisione.



■ Negozi Online ■ Servizi a venditori terzi ■ Amazon Web Services ■ Abbonamenti ■ Altro ■ Negozi Fisici

Fonte: Amazon Annual Report 2020, Amazon, 2020.

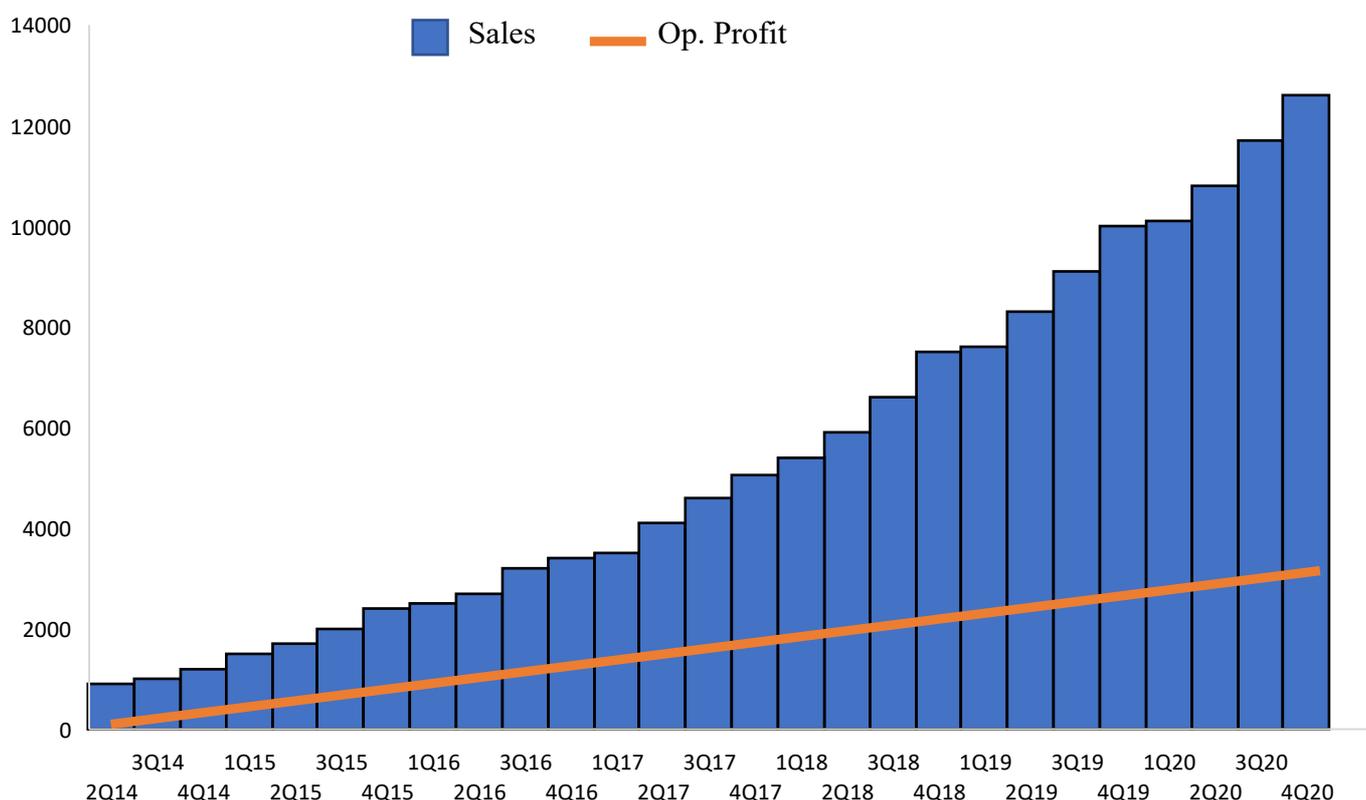
<sup>48</sup> Amazon Annual Report 2020, Amazon, 2020.

### 3.2.2 Amazon Web Services

Amazon Web Services, sezione di Amazon gestita da Andrew Jassy (ora CEO di Amazon, dopo le dimissioni di Jeff Bezos), rappresenta la principale fonte di utili per Amazon, è una piattaforma di *cloud computing e web services* lanciata nel 2006 per supportare Amazon.com.

Pur non rappresentando una grossa fetta dei ricavi, con il 13,2% del totale, vale il 59% dell'utile operativo [Grafico 37]. L'utile operativo, o EBIT, rappresenta quanto resta ad un'azienda del fatturato dopo aver coperto tutte le spese operative. Esso non include gli oneri finanziari, come tasse e debiti. Il risultato di Amazon Web Services è reso possibile dal fatto che, pur portando meno incassi, comporta costi molto bassi rispetto alle altre divisioni<sup>49</sup>.

Grafico 37 - Amazon Web Services trend di crescita dei ricavi e degli utili.



Fonte: Amazon Earnings Reports, in Millions Per Fiscal Quarter, AMAZON 2020

<sup>49</sup> Amazon: il bilancio del 2020, 19 aprile 2021, Starting Finance.

### 3.2.3 Infrastruttura globale di AWS e principali vantaggi

AWS *Cloud* opera in 81 zone di disponibilità, distribuite su 25 regioni geografiche in tutto il mondo, con altre 21 zone di disponibilità e 7 ulteriori Regioni AWS già annunciate in Australia, India, Indonesia, Israele, Spagna, Svizzera ed Emirati Arabi Uniti (EAU) [Figura 38].

Figura 38 - Posizione delle regioni di AWS.



Fonte: Amazon Web Services

L'infrastruttura globale di AWS è una delle principali piattaforme *cloud* a livello globale. Offre oltre 200 servizi completi di *data center* e possiede un ecosistema grande e dinamico, con milioni di clienti attivi e diversi *partner* in tutto il mondo. Il modello per regioni e zona di disponibilità di AWS è stato riconosciuto da Gartner come l'approccio ideale per eseguire applicazioni aziendali che richiedono un'elevata disponibilità<sup>50</sup>. I principali vantaggi dell'infrastruttura globale di AWS sono:

- Sicurezza

La sicurezza nei servizi *cloud* di AWS è garantita dall'infrastruttura centrale, che viene monitorata 24/7 per assicurare la riservatezza, l'integrità e la disponibilità dei dati dei clienti. Tutti i dati che passano attraverso la rete globale AWS che collega i vari *data center* e le regioni vengono automaticamente crittografati a livello fisico prima di lasciare le strutture sicure. I clienti di AWS hanno inoltre la possibilità di crittografare, spostare e gestire la *retention* dei dati.

<sup>50</sup> *Magic Quadrant for Cloud Infrastructure and Platform Services*, 27 luglio 2021, GARTNER.

- Disponibilità e Flessibilità

Ogni regione nell'infrastruttura di AWS è isolata e composta da più zone di disponibilità (porzioni isolate all'interno dell'infrastruttura). AWS permette ai clienti di isolare in modo più efficace ogni problematica e giungere ad una maggiore disponibilità e flessibilità: dà infatti la possibilità sia di scegliere quando e dove eseguire i carichi di lavoro e quando utilizzare la stessa rete, il piano di controllo, le API e i servizi AWS, sia di suddividere le applicazioni in più zone di disponibilità all'interno della stessa regione.

Inoltre, i piani di controllo AWS e la *console* di gestione AWS sono distribuiti su più regioni e includono *endpoint* API regionali, progettati per funzionare in sicurezza per almeno 24 ore se isolati dalle funzioni del piano di controllo globale senza richiedere ai clienti di accedere alla regione o ai propri *endpoint* API tramite reti esterne durante qualsiasi isolamento.

- Prestazione

Le regioni AWS sono in grado di offrire una latenza ridotta, una perdita di pacchetti minima e un'alta qualità della rete. Questo è reso possibile da una rete completa su fibra da 100 GbE. Le zone locali di AWS e AWS Wavelength, associate ai vari *provider* Telco, forniscono prestazioni adeguate alle applicazioni che richiedono latenze di pochi millisecondi, consegnando un'infrastruttura e dei servizi AWS più vicini agli utenti finali e ai dispositivi connessi in 5G.

- Servizio globale e Scalabilità

L'infrastruttura globale di AWS permette alle aziende di essere estremamente flessibili e di sfruttare la scalabilità del *cloud*. Solitamente i clienti stimavano un *provisioning* in eccesso per assicurarsi di avere la capacità sufficiente per gestire le operazioni aziendali ai massimi livelli di attività. Adesso possono effettuare il *provisioning* del numero di risorse di cui hanno effettivamente bisogno, sapendo che possono dimensionarsi istantaneamente rispetto alle effettive necessità aziendali. Questo porta ai clienti una riduzione dei costi, migliorando così la possibilità di rispondere alla domanda degli utenti.

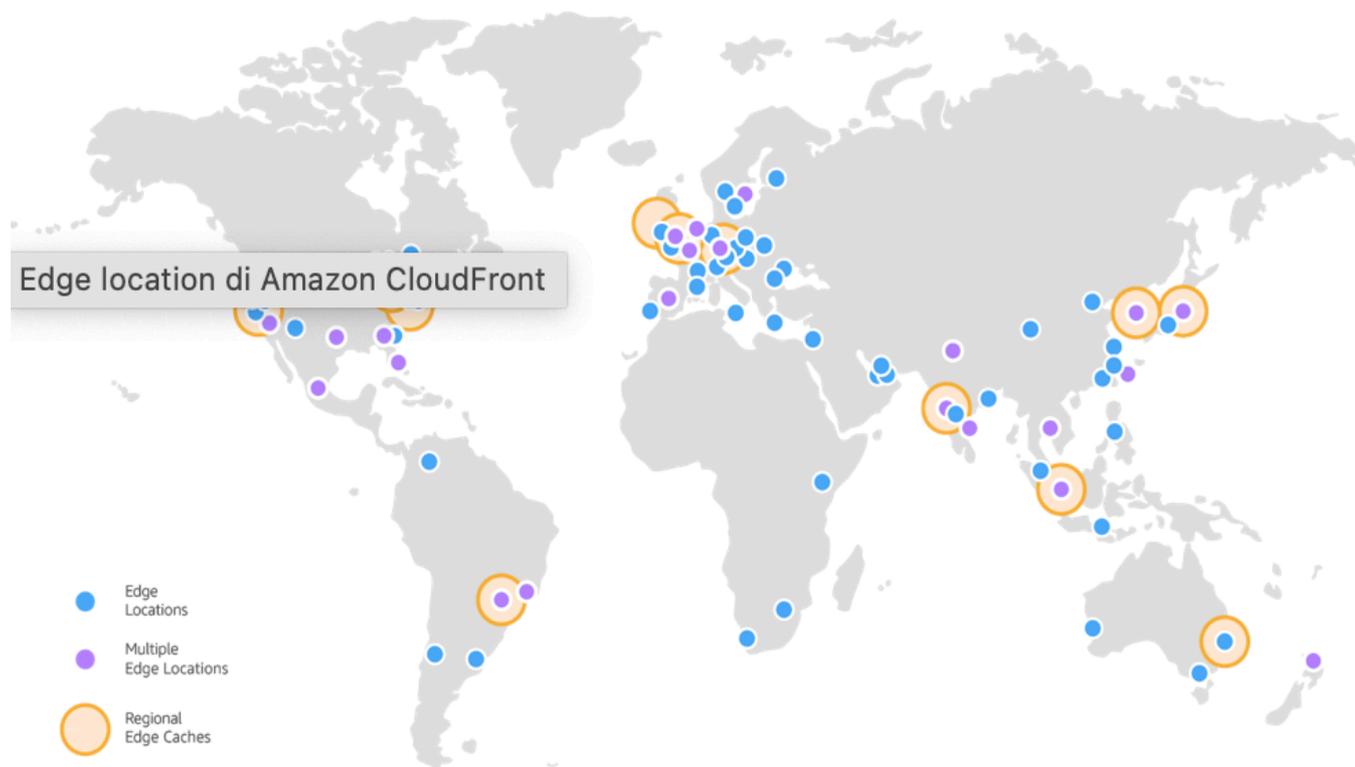
### 3.2.4 Principali servizi offerti da AWS

#### Amazon CloudFront

Amazon CloudFront è una rete per la distribuzione di contenuti o CDN (*Content Delivery Network*) che permette la distribuzione di dati, video, applicazioni e API a livello globale agli utenti con latenza minima e velocità di trasferimento elevata. Amazon CloudFront crea una connessione con diversi operatori di telecomunicazioni di livello 1/2/3 in tutto il mondo, è ben collegato con tutte le principali reti di accesso per garantire prestazioni ottimali e dispone di centinaia di *terabit* di capacità distribuita. Le *edge location* di CloudFront sono connesse alle regioni AWS attraverso la dorsale di rete AWS, costituita da una fibra parallela multipla da 100 GbE, completamente ridondante, che si estende su scala mondiale e collega diverse reti per garantire un migliore recupero dell'origine e l'accelerazione dei contenuti dinamici.

Per consentire la distribuzione di contenuti agli utenti finali con una bassa latenza, Amazon CloudFront impiega una rete globale di oltre 225 punti di presenza (più di 215 *edge location* e 13 *cache* regionali di livello intermedio) in 90 città e 47 paesi. La figura 39 mostra la posizione delle *edge location* di Amazon CloudFront.

Figura 39 - Edge location di Amazon CloudFront.



Fonte: Amazon Web Services

Opzioni di interconnessione:

- *Peering* pubblico: AWS è presente su 98 punti di scambio Internet pubblici. Alcuni di essi offrono circa mezzo *terabit* di capacità ciascuno. Le rotte verso determinati punti di scambio possono coincidere con le rotte offerte tramite l'interconnessione di rete privata.
- *Peering* privato: a seconda della posizione, o se un *peer* non può raggiungere AWS tramite un punto di scambio, potrebbe essere disponibile l'interconnessione di rete privata (PNI). I *peer* possono scegliere di connettersi a più dispositivi sull'*edge* AWS per garantire ridondanza e scalabilità.
- Collegamento diretto: *AWS Direct Connect* è una soluzione di servizi *cloud* che semplifica la creazione di una connessione di rete dedicata da una determinata posizione (ad esempio una sede aziendale) ad AWS. Utilizzando *AWS Direct Connect*, è possibile stabilire una connettività diretta e privata tra AWS e un *data center* specifico. Tale soluzione in molti casi può ridurre i costi di rete, aumentare il *throughput* della larghezza di banda e fornire un'esperienza di rete più coerente rispetto alle connessioni basate su Internet.

## Vantaggi di Amazon CloudFront

CloudFront offre diverse funzionalità di sicurezza, inclusa la crittografia a livello di campo e il supporto HTTPS, perfettamente integrati con AWS Shield, AWS Web Application Firewall (WAF) e Amazon Route 53 per proteggersi da diversi tipi di attacchi, inclusi attacchi DDoS a livello di rete e applicazione. Questi servizi si trovano in posizioni di *edge networking*, ridimensionati a livello globale e connessi tramite la dorsale di rete AWS. Sono in grado di fornire un'esperienza sicura, performante e disponibile. I principali vantaggi di Amazon CloudFront sono:

### 1. Sicurezza:

- Protezione da attacchi a livello di rete e applicazioni

Amazon CloudFront, AWS Shield, AWS WAF e Amazon Route 53 funzionano insieme per creare un perimetro di sicurezza flessibile, *multi-layer* contro tipologie multiple di attacchi, tra cui gli attacchi DDoS a livello di rete e applicazioni. Tutti questi servizi risiedono insieme nell'*edge* AWS e forniscono un perimetro di sicurezza scalabile, affidabile e a elevate prestazioni per le applicazioni e i contenuti. CloudFront funge da porta di ingresso per l'applicazione e l'infrastruttura, di conseguenza la superficie principale di attacco è lontana dai contenuti, dai dati, dal codice e dall'infrastruttura critici.

- Crittografie SSL/TLS e HTTPS

Con Amazon CloudFront, è possibile distribuire contenuti, API e applicazioni su HTTPS usando la versione più recente di *Transport Layer Security* (TLS, versione 1.3) in modo da crittografare e proteggere le comunicazioni tra i *client* dei visualizzatori e CloudFront.

- Controllo degli accessi

Con Amazon CloudFront è possibile limitare l'accesso ai contenuti utilizzando diverse funzionalità. Con URL e *cookie* firmati è possibile supportare l'autenticazione dei *token* per limitare l'accesso ai soli visualizzatori autenticati. Attraverso la restrizione geografica si può impedire agli utenti che si trovano in aree geografiche specifiche di accedere ai contenuti distribuiti tramite CloudFront.

## 2. Disponibilità

- *Origin Shield*

Le applicazioni *web* devono spesso affrontare picchi di traffico durante i periodi di intensa attività. Grazie ad Amazon CloudFront, il volume delle richieste dall'origine delle applicazioni si riduce automaticamente. I contenuti sono archiviati nelle *edge location* e nelle *cache* regionali di CloudFront e recuperati dalle origini all'occorrenza. È inoltre possibile ridurre ulteriormente il carico sulle origini delle applicazioni utilizzando *Origin Shield* per consentire un livello di *caching* centralizzato. *Origin Shield* ottimizza il rapporto di *hit cache* e concentra le richieste tra le regioni, consentendo una richiesta di origine per oggetto. Il traffico ridotto sulle origini consente di aumentare la disponibilità delle applicazioni.

- Abilitazione della ridondanza per le origini

CloudFront supporta diverse origini per la ridondanza dell'architettura *back-end*. La funzionalità di *failover* di CloudFront consente di distribuire automaticamente i contenuti da un'origine di *backup* nel caso in cui l'origine principale non sia disponibile.

## 3. *Edge Computing* altamente programmabile e sicuro

Amazon CloudFront offre funzionalità di calcolo *edge* CDN programmabili e sicure tramite CloudFront Functions e AWS Lambda@Edge.

- CloudFront Functions

CloudFront Functions è la soluzione per operazioni a scalabilità elevata e sensibili alla latenza, come manipolazioni delle intestazioni HTTP, riscritture/re-indirizzamenti di URL e normalizzazioni della chiave di *cache*. Questi tipi di operazioni di breve durata permettono di gestire il traffico spesso imprevedibile e con dei picchi.

- Lambda@Edge

AWS Lambda@Edge è una funzionalità di calcolo *serverless* per utilizzo generico che supporta un'ampia gamma di personalizzazioni ed esigenze di calcolo. Lambda@Edge può essere utilizzato per operazioni a elevata intensità di calcolo, come le elaborazioni che richiedono più tempo per il completamento (da diversi millisecondi a secondi) o chiamate di rete per l'elaborazione dei dati.

## **AWS Wavelength**

AWS Wavelength è un'infrastruttura AWS che offre applicazioni ottimizzate per l'*edge computing mobile*. Le zone di Wavelength sono infrastrutture AWS distribuite che integrano i servizi di calcolo e lo *storage* di AWS nei *data center* dei fornitori di servizi di telecomunicazione a livello di *edge* della rete 5G, permettendo al traffico delle applicazioni da dispositivi 5G di raggiungere i *server* delle applicazioni in esecuzione nelle zone Wavelength senza uscire dalla rete delle telecomunicazioni. Ciò permette di evitare che la latenza che risulterebbe dal traffico delle applicazioni debba attraversare più *hop* in Internet per raggiungere la destinazione, permettendo ai clienti di sfruttare totalmente i vantaggi della latenza e della larghezza di banda offerti dalle reti 5G moderne. Le zone di AWS Wavelength sono disponibili in dieci città degli Stati Uniti sulla rete 5G di Verizon, a Tokyo e Osaka, in Giappone, sulla rete KDDI 5G, a Daejeon, Corea del Sud, sulla rete 5G di SK Telecom e a Londra sulla rete 5G di Vodafone.

AWS Wavelength permette alle applicazioni 5G di offrire esperienze interattive e coinvolgenti, come lo *streaming* di giochi, la realtà virtuale e le esperienze in sede per eventi dal vivo. Wavelength consente anche di scaricare i lavori di elaborazione dei dati da dispositivi 5G nell'*edge* della rete per conservare risorse come l'alimentazione, la memoria e la larghezza di banda, che rendono le applicazioni veicoli autonomi e *smart*.

## **AWS Global Accelerator**

AWS Global Accelerator è un servizio di rete che migliora le prestazioni del traffico degli utenti fino al 60% attraverso l'infrastruttura di rete globale di Amazon Web Services. Quando Internet è congestionato, le ottimizzazioni dell'instradamento automatico di AWS Global Accelerator contribuiscono a mantenere uniformemente bassi i valori di perdita di pacchetti, *jitter* e latenza. AWS Global Accelerator contribuisce a ridurre il divario tra le distribuzioni in una singola regione e in molteplici regioni migliorando l'instradamento di rete del traffico utente locale e globale. Se il traffico diretto alla singola regione di un'applicazione viene lasciato sulla rete Internet pubblica, può subire ripercussioni negative dovute alla congestione di Internet e alle interruzioni locali. Utilizzando Global Accelerator, il traffico degli utenti viene trasferito da Internet alla rete globale privata di Amazon attraverso oltre 90 *edge location* a livello globale, e successivamente indirizzato alle origini delle applicazioni. AWS Global Accelerator si configura rapidamente e migliora le prestazioni del traffico fino al 60%. Con Global Accelerator l'utente avrà a disposizione due IP globali statici che agiscono come punto di accesso fisso per un'applicazione, migliorando la disponibilità.

## Sicurezza

### AWS WAF

AWS WAF è un *firewall* per applicazioni *web* che aiuta a proteggere le applicazioni *web* o le API dagli *exploit web* che possono intaccare la disponibilità delle applicazioni, compromettere la sicurezza o consumare risorse eccessive. Grazie ad AWS WAF è possibile controllare il modo in cui il traffico raggiunge le applicazioni, permettendo di creare regole di sicurezza che controllano il traffico dei *bot* e bloccano i comuni *pattern* di attacco, come *SQL injection* o *cross-site scripting*. Inoltre, è possibile personalizzare le regole che filtrano *pattern* di traffico specifici. È possibile inserire AWS WAF in Amazon CloudFront nell'ambito di una soluzione CDN.

### AWS Shield

AWS Shield è un servizio di protezione da attacchi di tipo DDoS (*Distributed Denial of Service*) che protegge le applicazioni in esecuzione in AWS. AWS Shield fornisce un rilevamento continuo e una prevenzione incorporata automatica che minimizzano il tempo di inattività e la latenza dell'applicazione, così che non è necessario ricorrere ad AWS Support per beneficiare della protezione DDoS. Esistono due livelli di AWS Shield: *Standard* e *Advanced*. Tutti i clienti AWS beneficiano delle funzionalità di protezione automatica di AWS Shield *Standard*, senza costi aggiuntivi. AWS Shield *Standard* protegge dagli attacchi DDoS di rete e di livello trasporto più comuni e frequenti a siti *web* o applicazioni. Chi utilizza AWS Shield *Standard* con Amazon CloudFront e Amazon Route 53, potrà avvalersi della protezione completa contro tutti gli attacchi a livello di infrastruttura (livello 3 e 4).

### 3.2.5 CloudFront per lo *streaming* video in diretta e *on-Demand*<sup>51</sup>

CloudFront è progettato per gestire i carichi di lavoro relativi ai video in diretta e *on-demand* attraverso la rete AWS scalabile e dalle prestazioni globali, la connettività della dorsale privata alle origini AWS e l'integrazione con AWS ed Elemental Media Services.

#### *Streaming on-demand*

Figura 40 - Struttura della distribuzione dei contenuti per i servizi VOD.



#### **Workflow Example: Content Distribution for VOD Services**

Fonte: *Amazon CloudFront for Media: Best Practices for Streaming Media Delivery*

Nel caso dello *streaming on-demand*, il contenuto del video viene memorizzato su Amazon S3 e gli utenti possono decidere di guardare il contenuto in qualsiasi momento. Normalmente una soluzione completa di *streaming on-demand* utilizza Amazon S3 per l'archiviazione, AWS Elemental Media Converter per l'elaborazione di video basata su *file* e Amazon CloudFront per la distribuzione [Figura 40]. Amazon S3 è una struttura di archiviazione di risorse video, è scalabile, ha una ridondanza incorporata e offre tariffe basate sul consumo effettivo.

Una volta che il contenuto viene caricato, potrebbe essere necessario convertire il video nella dimensione, risoluzione o formato supportati da un televisore particolare o da un dispositivo collegato.

AWS Elemental MediaConvert si occupa di questo. MediaConvert prende il contenuto da S3, lo transcodifica in base alla richiesta e memorizza il nuovo risultato in S3. La transcodifica elabora i *file* video, creando versioni compresse del contenuto originale per ridurre le dimensioni, modificarne il formato o aumentare la compatibilità con i dispositivi di riproduzione. Una volta che i contenuti sono archiviati in modo sicuro e sono disponibili nei formati richiesti dagli utenti, la loro distribuzione a livello mondiale avviene con Amazon CloudFront. La rete per la distribuzione di contenuti di Amazon memorizza il contenuto nelle *edge location* per una latenza minima e una velocità di trasmissione video elevata.

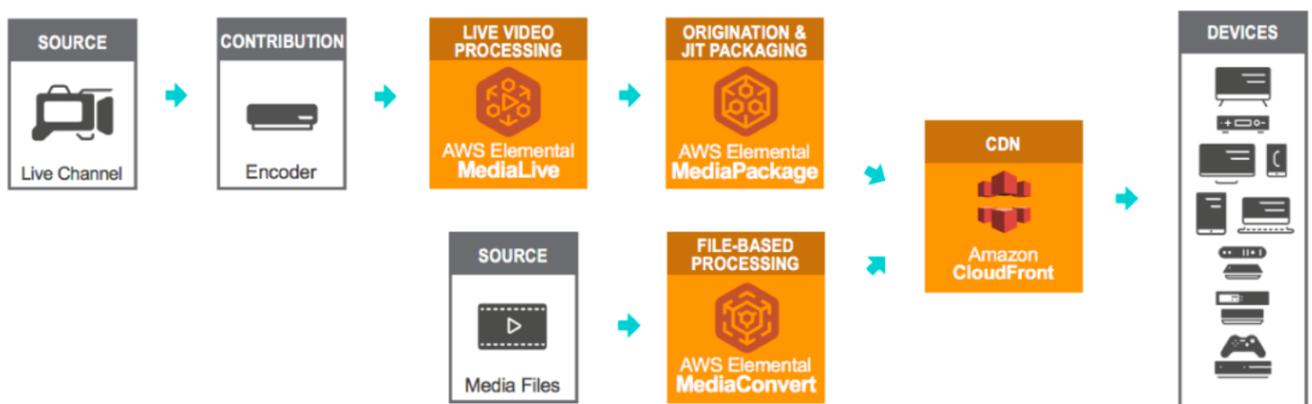
<sup>51</sup> *Amazon CloudFront for Media: Best Practices for Streaming Media Delivery*, novembre 2020, white paper, Amazon.

## Diretta streaming

Figura 41 - Struttura della distribuzione dei contenuti per le dirette streaming.



### Workflow Example: Large-scale Live Events



### Workflow Example: 24x7 Live Channel Delivery

Fonte: Amazon CloudFront for Media: Best Practices for Streaming Media Delivery

Nel caso della diretta *streaming*, i contenuti possono riguardare eventi in diretta o la trasmissione di canali in diretta 24 ore su 24, 7 giorni su 7. Tra gli esempi del primo figurano le emittenti e gli aggregatori di contenuti che trasmettono in *streaming* tornei sportivi, cerimonie di premiazione, discorsi programmatici e altri eventi dal vivo molto seguiti. Esempi del secondo tipo sono gli studio, le emittenti e gli operatori di servizi di *pay TV* che desiderano pacchettizzare e trasmettere canali lineari in diretta su Internet direttamente al loro pubblico, senza una piattaforma di distribuzione di terzi.

È possibile utilizzare AWS per trasmettere contenuti in diretta a un pubblico mondiale. Il primo passo è l'elaborazione del video in diretta e a tal fine è possibile utilizzare AWS Elemental MediaLive, che codifica la diretta *streaming* del video in tempo reale prendendo una sorgente video in diretta di grandi dimensioni (ad esempio, proveniente da un codificatore locale come AWS Elemental Live) e comprimendola in versioni più piccole da distribuire agli utenti. Il secondo passo prevede due opzioni a seconda dei casi specifici.

È possibile utilizzare un pacchetto di origine JIT come AWS Elemental MediaPackage per convertire il contenuto video da un singolo formato in più formati e pacchettizzarlo in modo sicuro per diversi tipi di dispositivi. MediaPackage rende più semplice implementare caratteristiche video molto popolari tra gli utenti (autoplay, pausa, rewind, ecc.), come quelle che è possibile trovare nei videoregistratori digitali. Inoltre, consente di proteggere i contenuti utilizzando sistemi di *Digital Rights Management* (DRM). In alternativa, se il codificatore sta già trasformando il contenuto nel formato richiesto da tutti i dispositivi degli utenti finali, è possibile utilizzare un'origine scalabile ad alte prestazioni come AWS Elemental MediaStore [Figura 41].

MediaPackage e MediaStore distribuiscono il contenuto su Amazon CloudFront, che lo indirizzerà al pubblico che sta guardando l'evento in diretta.

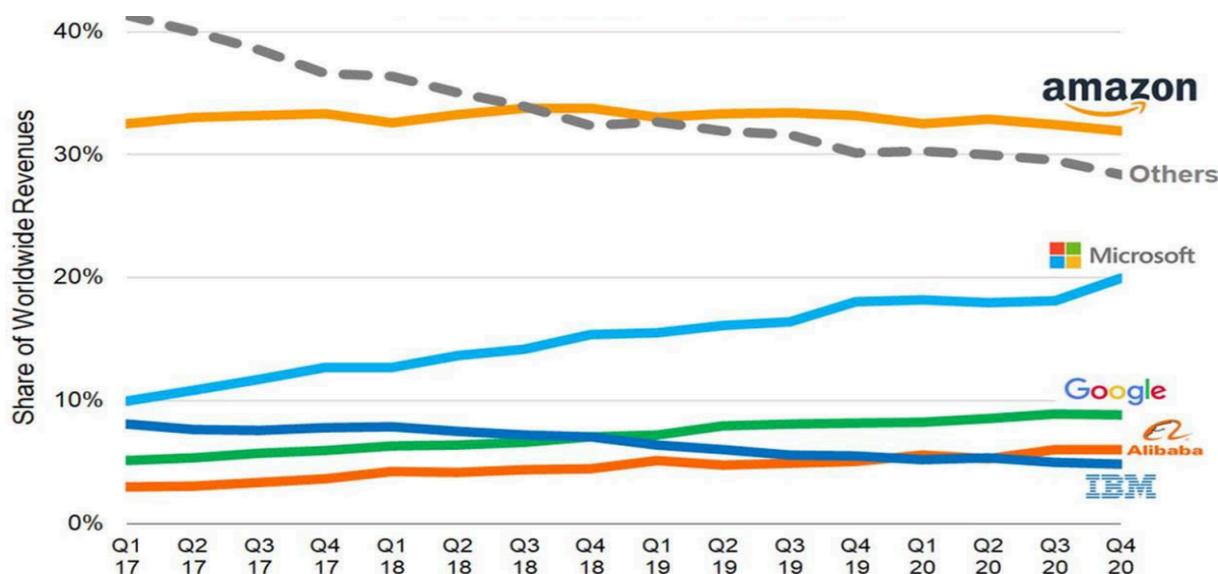
Una volta che la soluzione è pronta e viene eseguita, l'evento in diretta può essere trasmesso in tutto il mondo in modo scalabile ed economico. La CDN può ospitare un pubblico che varia per dimensioni ed è in grado di gestire "affollamenti lampo".

### 3.2.6 Panoramica di mercato dei *Cloud Infrastructure & Platform Services (CIPS)*

Il mercato mondiale dei CIPS (*Cloud Infrastructure & Platform Services*), in cui Amazon si inserisce, è dominato in gran parte da quattro *player*: Alibaba Cloud in Cina e nei paesi asiatici circostanti, AWS, Google e Microsoft nel resto del mondo.

I *provider non hyperscale* sono stati in gran parte relegati a scenari specializzati, che richiedono un supporto approfondito per le tecnologie *legacy* o che hanno requisiti di posizione specifici che non possono essere soddisfatti da un *provider cloud hyperscale*. In generale, i *provider hyperscale* offrono un'ampia gamma di funzionalità e possono soddisfare i requisiti aziendali di disponibilità, prestazioni, sicurezza, conformità normativa, servizio e supporto.

Grafico 42 - Trend della quota di mercato dei fornitori di servizi Cloud (IaaS, PaaS, Hosted Private Cloud).



Fonte: Synergy Research Group

La maggior parte delle aziende ha adottato CIPS in modo strategico e dispone di un'ampia gamma di carichi di lavoro su IaaS e PaaS, comprese le applicazioni di produzione. Le aziende di fascia media sono le più propense a credere che i servizi *cloud*, come IaaS, sostituiranno quasi tutte le loro infrastrutture di *data center* nei prossimi cinque anni. Nel mercato sono disponibili offerte sia pubbliche che private, tuttavia, la distinzione tra IaaS *cloud* pubblico e privato è molto sottile, poiché i *provider* CIPS estendono le loro regioni in *data center* aziendali e *Edge location*. Si sta quindi affermando il cosiddetto “*cloud distribuito*”, che si riferisce alla distribuzione di servizi di *cloud* pubblico in diverse sedi fisiche, che possono includere *data center* aziendali, mentre il funzionamento, la *governance*, gli aggiornamenti e l'evoluzione dei servizi sono di responsabilità del *provider* del *cloud* pubblico di origine. Il *cloud distribuito* abilita una caratteristica chiave delle operazioni in *cloud*: elaborazione a bassa latenza in cui le operazioni di elaborazione per i servizi *cloud* sono più vicine a coloro che necessitano delle funzionalità. Ciò può fornire importanti miglioramenti delle prestazioni e può ridurre il rischio di interruzioni legate a disfunzioni della rete globale.

### 3.2.7 AWS punti di forza e debolezza/criticità

Nell'attività *cloud*, Amazon ha riportato nel 2020 una crescita delle vendite del 34% anno su anno, pari a 9,95 miliardi di dollari, e al di sopra delle attese di mercato. Il risultato rappresenta tuttavia un lieve rallentamento rispetto al terzo trimestre quando i ricavi di AWS sono cresciuti del 35%. L'utile operativo di AWS è di 2,6 miliardi, +19% anno su anno e sopra le previsioni di mercato (2,45 miliardi). Amazon sta continuando a investire costruendo nuovi *data center* e assumendo ingegneri per contrastare la forte concorrenza di Microsoft e Google che nel *cloud* stanno conquistando ampie fette di mercato.

Punti di forza:

- AWS continua ad avere un ruolo guida in molte delle dimensioni critiche del mercato CIPS, inclusa la quota di mercato totale e le capacità delle offerte. AWS detiene la quota maggiore del mercato mondiale nelle offerte IaaS e PaaS di *database*.
- AWS ha le competenze, le risorse e la motivazione per integrare verticalmente e fornire soluzioni *end-to-end* ai clienti. L'azienda può progettare qualsiasi cosa, dal silicio nei suoi *server* ai sistemi operativi incorporati nei dispositivi perimetrali e l'intero *stack* di *software* in mezzo.
- AWS è un'azienda estremamente ben gestita dal punto di vista finanziario e genera oltre il 50% del reddito operativo per tutta Amazon. A differenza di altri fornitori presenti nel *Magic Quadrant* di Gartner [Figura 43], i buoni margini di AWS sono destinati a migliorare la società madre.

Criticità:

- Le crescenti preoccupazioni circa le dimensioni e la portata di Amazon, insieme alla posizione di *leadership* di AWS, mettono in *stand-by* le relazioni con alcuni dei suoi *partner* e clienti. Inoltre, AWS rischia di alienare gli sviluppatori di *software* a causa delle schermaglie dell'azienda con le comunità di *software open source* (OSS). In particolare, un'ampia gamma di offerte AWS ha beneficiato di OSS, senza alcun contributo materiale in natura da parte di AWS.
- AWS ha una scarsa coesione tra i suoi *set* di offerte in continua espansione. La posizione di *leadership* dell'azienda in IaaS e dbPaaS crea un effetto fuorviante per le altre offerte/servizi. Il *design* organizzativo di AWS che consente ai suoi sviluppatori di operare come unità semiautonome crea incongruenze tra i prodotti, piuttosto che un insieme coeso, in particolare per i nuovi servizi. Inoltre, l'uso efficace di AWS richiede la mentalità di un costruttore di applicazioni e, se associato a una scarsa coesione, può essere scoraggiante per molte aziende.

- I clienti continuano a credere erroneamente che AWS riduca ampiamente i prezzi; tuttavia, le diminuzioni spesso non sono applicate universalmente a tutti i servizi. Ad esempio, lo *storage* con *provisioning* per il servizio di elaborazione di AWS non ha subito una riduzione di prezzo dal 2014, quasi la metà della vita dell'azienda, nonostante i prezzi siano diminuiti drasticamente nel mercato per i componenti grezzi.

Figura 43 - Magic Quadrant per l'infrastruttura cloud e i servizi di piattaforma.



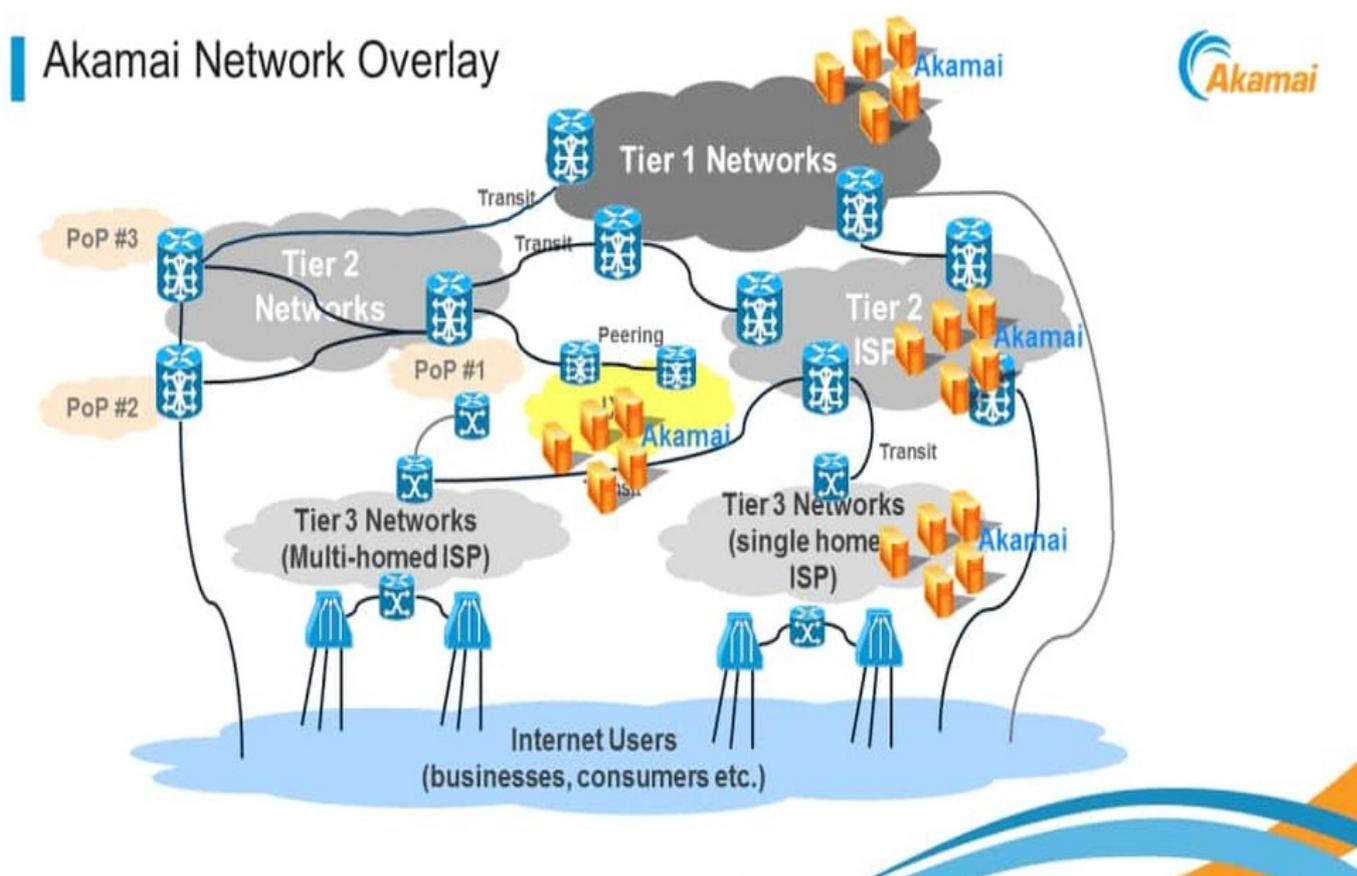
Fonte: Magic Quadrant for Cloud Infrastructure and Platform Services, 27 luglio 2021, GARTNER.

### 3.3 AWS CloudFront vs Akamai CDN

Entro il 2022, i video *online* costituiranno oltre l'82% di tutto il traffico Internet per gli utenti. Lo *streaming* video in diretta, in particolare, sta esplodendo in popolarità. Oggi esistono reti di *content delivery* che facilitano la distribuzione dei contenuti, spostando i dati in vaste regioni geografiche, per raggiungere gli spettatori di tutto il mondo. Questa tecnologia è assolutamente essenziale nel mondo dello *streaming* video *online*. I *file* video sono notoriamente ingombranti, quindi un sistema affidabile per la consegna è un *must*. Sia Akamai che AWS CloudFront sono piattaforme potenti, ma quale di queste piattaforme è migliore per lo *streaming* video in diretta?

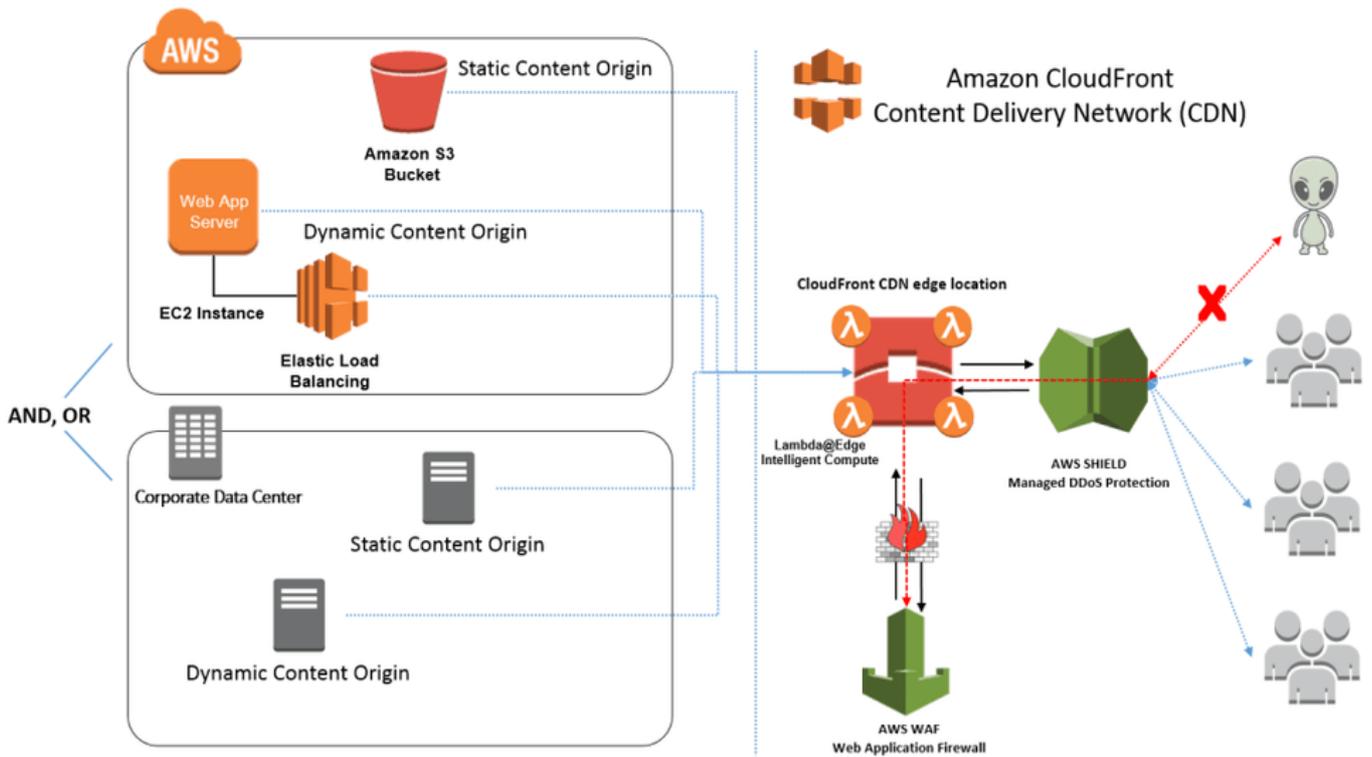
La rete CDN di *streaming* video di Akamai è composta da oltre 240.000 *server* situati in tutto il mondo.

Figura 44 - Piattaforma CDN di Akamai.



Fonte: Akamai.com

Figura 45 - Piattaforma CDN di AWS.



AWS CloudFront è una CDN fornita da Amazon. *Fonte: AWS CloudFront*

#### - Scalabilità

Una delle metriche più importanti per una CDN di *streaming* video è la dimensione della rete. Più grande è la rete di cui si dispone più sono gli *endpoint* a cui è possibile indirizzare gli utenti, determinando una maggiore vicinanza all'*end-user*, il che riduce la congestione e migliora notevolmente l'esperienza dell'utente (QoE). Akamai dispone di *server* in più di 130 paesi collegati a più di 1.700 reti. CloudFront, d'altra parte, ha più di 225 PoP. Poiché i *file* video sono di grandi dimensioni, avere più *server* distribuiti strategicamente è un grande vantaggio nella distribuzione di *streaming online*. La differenza tra Akamai e AWS CloudFront è significativa in questo campo.

#### - Performance

La velocità di una CDN non può essere misurata semplicemente utilizzando un numero. Le prestazioni dipendono da chi esegue il *test*, da dove si trova, dalla congestione della rete in quel momento, dalla velocità di Internet dell'utente, da altre applicazioni in esecuzione, da attacchi informatici simultanei e così via. Tuttavia, dalle analisi emerge che Akamai sembra avere un netto vantaggio su CloudFront quando si tratta di prestazioni.

La velocità di trasmissione di una CDN è una buona metrica per esaminare le prestazioni dello *streaming* video in diretta. In un'analisi del *throughput* CDN, Akamai è circa il 14% più veloce di CloudFront. I test internazionali tendono inoltre a mostrare un vantaggio di velocità del 15-20% per Akamai grazie alla sua più ampia distribuzione globale. Ciò è particolarmente importante per lo *streaming live* in quanto riduce i problemi di visualizzazione, come ad esempio i problemi di *buffering*.

#### - Affidabilità

Ci sono due componenti principali da considerare quando si tratta di determinare l'affidabilità: disponibilità e sicurezza. Per quanto riguarda la disponibilità, la rete di Akamai si attesta al 99,77% secondo CDN Finder, mentre CloudFront si attesta al 99,74%. La differenza tra i due è insignificante. È noto che AWS è in ritardo rispetto alla maggior parte dei CDN quando si tratta di sicurezza. Tuttavia, AWS CloudFront ha ulteriormente sviluppato le sue offerte e i suoi servizi di sicurezza per includere le crittografie SSL/TLS e il controllo degli accessi, infatti è conforme ai principali *standard* di sicurezza dei *media*. Akamai, d'altro canto, è *leader* di mercato nella distribuzione sicura dei contenuti ed è stata la prima rete CDN a offrire protezione DDoS e WAF. Il servizio Kona Site Defender protegge da una vasta gamma di minacce. In genere, le offerte di sicurezza di Akamai sono gestite da professionisti interni esperti, che richiedono poca configurazione e interazione da parte degli utenti.

#### - Prezzo

I prezzi di CloudFront sono relativamente aggressivi. Hanno una struttura semplice, con pagamento in base al consumo, anche se ci sono molti costi aggiuntivi, che devono essere presi in considerazione. Akamai ha un sistema di prezzi più complesso, che si basa su contratti negoziati. Non è trasparente. Il prezzo dipende dalla larghezza di banda, dall'area geografica, dai tipi di traffico e dalla durata del contratto.

Quindi, in conclusione ci sono diversi motivi per cui Akamai è migliore di AWS CloudFront per le piattaforme di *live streaming* professionali quando viene analizzato in base a scalabilità, prestazioni, affidabilità e prezzi. Non ci sono dubbi, quindi, che Akamai sia il *leader* di mercato nel contesto delle CDN con una quota di mercato del 35% basata sul fatturato annuo a livello globale. Essa serve la maggior parte delle aziende *Fortune* 500. AWS CloudFront offre comunque soluzioni molto potenti adatte per l'*hosting* di siti *web* professionali e la distribuzione di contenuti.

### 3.4 Limelight Networks

Limelight Networks è un'azienda americana quotata (NASDAQ) fondata nel 2001 a Tempe, in Arizona, che fornisce un servizio di rete di distribuzione di contenuti (CDN), utilizzato per la distribuzione di contenuti multimediali digitali e *software*. A febbraio 2020, la rete dell'azienda è formata da più di 130 punti di presenza (POP) e offre oltre 70 *terabit* al secondo di capacità in uscita in tutto il mondo.

Limelight è uno dei principali fornitori di servizi di distribuzione dei contenuti (CDN) che consente alle organizzazioni di godere di siti *web* più veloci, applicazioni più reattive, video di altissima qualità e *download* di giochi e *software* su qualsiasi dispositivo. Man mano che emergono nuove tendenze digitali come la distribuzione di video OTT, aggiornamenti quotidiani di *software* e applicazioni e strategie di distribuzione multiplatforma, Limelight dà la possibilità alle aziende grazie ai propri servizi e alle proprie infrastrutture di fare affari *online* con maggiore velocità, affidabilità e sicurezza. L'architettura di rete di Limelight può supportare in modo univoco sia i *file* di piccole dimensioni che i *file* di grandi dimensioni, che comprendono la maggior parte dei contenuti come video, *software* e giochi. L'architettura e i servizi che Limelight è in grado di offrire sono:

- Una rete di POP globali che mette i contenuti offerti da una determinata piattaforma alla portata di qualsiasi utente.
- Un potente *software* in grado di ottimizzare i contenuti per la migliore esperienza di visualizzazione su qualsiasi dispositivo.
- Servizi *cloud* integrati *end-to-end* dallo *storage* alla consegna accelerata.

L'offerta di Limelight si concentra quindi su due principali soluzioni:

1. *Edge Cloud*: A differenza dei tradizionali fornitori di servizi *cloud* che si affidano alla congestionata rete Internet pubblica per trasferire i dati critici, Limelight utilizza una delle reti private più grandi del mondo, con una portata e una scalabilità globali che riducono al minimo le latenze. Limelight's *Edge Cloud* elimina i costi e la complessità di utilizzo degli ambienti di *cloud computing* tradizionali per applicazioni di *edge computing* e IoT a bassa latenza. All'interno di tale soluzione si inserisce Limelight Real Time *Streaming*, che fornisce agli utenti, ovunque si trovino, uno *streaming* video *live* in meno di un secondo. Limelight Realtime *Streaming* utilizza la tecnologia *standard* del settore WebRTC, aperta e scalabile, per fornire uno *streaming* video in tempo reale, affidabile e di qualità *broadcast*, utilizzando il protocollo di trasferimento dati UDP.

2. Sicurezza nel *Cloud*: I servizi di sicurezza nel *cloud* di Limelight offrono una difesa a più livelli contro gli attacchi malevoli ai siti *web* e l'accesso non autorizzato ai contenuti, senza influire sulle prestazioni delle applicazioni *web* e sulla distribuzione dei contenuti stessi. Limelight DDoS Attack Interceptor protegge dagli attacchi di tipo *denial of service* destinati a sovraccaricare i servizi *online* con grandi volumi di traffico malevolo. Limelight Web Application Firewall protegge i siti *web* e le applicazioni *web* dagli attacchi malevoli a livello di applicazione *http*, che mirano a compromettere il sito *web* e a sottrarre i dati. Le funzionalità TLS/SSL crittografano i dati per evitare che possano essere intercettati durante il transito e sono disponibili diverse soluzioni di sicurezza per i contenuti, in modo che solo gli utenti autorizzati vi abbiano accesso. Limelight offre una gamma scalabile di soluzioni di sicurezza nel *cloud* che proteggono l'infrastruttura e i contenuti senza influire sulle prestazioni.

### 3.5 Fastly<sup>52</sup>

Fastly è stata fondata a San Francisco nel 2011 da Artur Bergman. Nel settembre 2015, Google ha unito le forze con Fastly e altri fornitori di CDN per offrire servizi CDN ai propri utenti. Nell'aprile 2017, Fastly ha introdotto la sua piattaforma *cloud edge* perimetrale, che fornisce una rete di distribuzione dei contenuti (CDN), servizi di sicurezza Internet, bilanciamento del carico, servizi video e *streaming* e un *firewall* per applicazioni *web* (WAF). L'architettura di Fastly è formata da migliaia di punti di presenza (POP) piccoli e sparsi. Internet sta diventando sempre più dinamico e Fastly ha adottato un approccio diverso: ha concentrato gli sforzi sul posizionamento di meno POP più potenti nei mercati strategici di tutto il mondo (gli unici *multiple POP* sono a Chicago, New York, San Jose, Francoforte, Londra, Singapore, San Paolo, Tokyo, Atlanta, Ashburn, Dallas, Los Angeles). Grazie al transito Tier 1, a *server* alimentati da unità a stato solido (SSD) e a un *team* di ingegneri il cui obiettivo è ottimizzare la velocità, Fastly ha creato una rete veloce che richiede meno *hardware* per fornire una portata globale completa ed assicurare una migliore esperienza utente (QoE). L'offerta di Fastly si concentra su 3 diverse soluzioni:

#### 1. *Delivery*

La piattaforma Fastly Deliver Edge è una rete globale, sicura e scalabile. È formata da POP strategicamente distribuiti e ad alte prestazioni per aiutare i clienti a spostare dati e applicazioni più vicino agli utenti e fornire rapidamente contenuti aggiornati. La rete Fastly è costruita per supportare le esigenze di *streaming* più

---

<sup>52</sup> “*More confidence. More speed. More power at the edge. Build, secure, and deliver more powerful websites and applications with Fastly's edge cloud platform.*” Fonte: Fastly.com

esigenti, è completamente configurabile, sicura e garantisce risparmio ed efficienza. Mettendo più *cache* all'*edge* e riducendo al minimo i viaggi verso l'origine, l'architettura Deliver Edge può aiutare a ridurre i costi di infrastruttura. La CDN altamente configurabile di Fastly dà la libertà di controllare come i contenuti vengono memorizzati nella *cache* in modo da poterli fornire rapidamente agli utenti che li desiderano. La consegna in *streaming* a bassa latenza, con eventi di *rebuffering* minimi, è la chiave per fornire esperienze video di qualità *broadcast* su qualsiasi dispositivo. La piattaforma *cloud* perimetrale di Fastly è progettata per garantire elevate prestazioni: con una capacità in crescita di oltre 130 Tbp, si adatta per soddisfare le esigenze dei più grandi servizi di *streaming* e video del settore.

## 2. Sicurezza

Fastly è in grado di assicurare soluzioni di sicurezza in grado di mantenere i siti *web* sicuri e performanti, consentendo alle organizzazioni di rilevare efficacemente le minacce prima che abbiano un impatto sulle attività. Le offerte DDoS, WAF e TLS di nuova generazione forniscono la protezione e il controllo necessario alle aziende, senza sacrificare le prestazioni. Le soluzioni *web* Application Firewall (WAF) e Runtime Application Self Protection (RASP) di nuova generazione proteggono l'intero portafoglio di applicazioni delle organizzazioni e forniscono la visibilità necessaria che consente ai *team* DevOps di rendere le loro applicazioni più resilienti. Le innovazioni e l'efficienza delle soluzioni proposte da Fastly sono state premiate più volte dagli analisti del settore: Gartner ha riconosciuto due volte il WAF di nuova generazione (ex Signal Sciences) nel Gartner Magic Quadrant per WAF.

## 3. Compute

L'offerta *Compute Edge* di Fastly consente di creare applicazioni su larga scala e distribuite a livello globale e di eseguire codice all'*edge*, senza dover gestire l'infrastruttura sottostante. Permette alle organizzazioni di distribuire ed eseguire logiche complesse per qualsiasi applicazione o servizio di *backend*, assicurando un approccio sicuro, performante e scalabile. A 35,4 microsecondi, la soluzione *Compute Edge* di Fastly fornisce un tempo di avvio per l'esecuzione del codice 100 volte più veloce rispetto ad altre soluzioni *serverless*. Garantisce al cliente la possibilità di eseguire il suo codice su centinaia di *server* situati in tutto il mondo contemporaneamente. Operando in pochi microsecondi, la tecnologia di isolamento di Fastly aiuta a proteggere dagli attacchi e garantire prestazioni di livello. Creando e distruggendo un *sandbox* per ogni richiesta che arriva attraverso la piattaforma, si limita il raggio di "esplosione" del codice difettoso o degli errori di configurazione da parte di altri utenti, riducendo quindi la superficie di attacco. La QoE è uno dei principali obiettivi nella trasformazione digitale e la piattaforma *cloud edge* di Fastly consente agli sviluppatori di eseguire, proteggere e distribuire siti *web* e applicazioni, il più vicino possibile agli utenti, per garantire una QoE elevata su scala globale.

### 3.6 Mainstreaming

È il pioniere della nuova generazione di *Global Video Delivery Network* con sede in Italia e nella Silicon Valley, fondata nel 2016 da Antonio Corrado (CEO), Philippe Tripodi (COO) e Giovanni Proscia (CTO), permette di distribuire video *real-time* su Internet. Mainstreaming nasce con l'obiettivo di innovare il settore del *Content Delivery Network* e si specializza nella distribuzione di contenuti video in *real time*, come il *live streaming*, basati su una tecnologia proprietaria e un'architettura tecnologica messa a punto nel centro R&D di Milano. La società ha creato un algoritmo che è in grado di distribuire video alla massima qualità anche in presenza di un'*audience* molto ampia, di utenti contemporanei e con una notevole riduzione del consumo energetico, di gran lunga inferiore alle tecnologie Internet tradizionali. La tecnologia innovativa di MainStreaming nasce per soddisfare mercati emergenti come le OTT TV (*Over the Top Television*) ed offre ai *Broadcaster* tradizionali l'opportunità di migrare i loro contenuti su IP. Il servizio di *Video Delivery Network* è rivolto sia ai grandi *Broadcaster* globali, OTT TV (*Over-the-top TV*) e *Digital Media Company*, garantendo un servizio di *Video Delivery* ad alta qualità e *performance* elevate, sia a *Media Company* emergenti, *Publisher* e *Broadcaster* locali, supportandoli in tutte le funzionalità di *encoding*, gestione e distribuzione di contenuti video. Infine, le soluzioni di MainStreaming sono ideali per i *player* dell'eSport in *live streaming*, per le *media company* di intrattenimento e per i giocatori *online* a livello competitivo. MainStreaming si posiziona nel mercato delle *Content Delivery Network* (CDN) anche se fa parte della nuova generazione delle *Video Delivery Network*.

I suoi *competitors* principali sono appunto Akamai, LimeLight e Fastly. I vantaggi di MainStreaming rispetto ai *competitor* sono tre:

1. Sistema senza *caching*.

Per ogni video da distribuire vengono generate solo poche copie, non centinaia o migliaia come nei servizi di CDN tradizionali, garantendo una notevole riduzione di consumo energetico e l'impiego di meno *server*.

2. È specializzata esclusivamente nella distribuzione video.

Rispetto ai servizi tradizionali multi *purpose*, MainStreaming è specializzata esclusivamente nella distribuzione del video garantendo una trasmissione con alte *performance* ed una migliore *User Experience*.

3. L'algoritmo proprietario.

È in grado di distribuire video alla massima qualità anche in presenza di numerosi utenti contemporanei, poiché la rete e la tecnologia di *delivery* sono stati concepiti per la diffusione del video in *Real Time*.

Con il nuovo algoritmo, MainStreaming si inserisce in un mercato, quello del video *online*, in forte crescita.

## **La piattaforma iMDP (*intelligent Media Delivery Platform*)**

MainStreaming è una società di distribuzione multimediale intelligente che consente ai *media*, alle imprese e alle società di gioco di garantire la migliore qualità di esperienza al proprio pubblico, attraverso la rivoluzionaria tecnologia basata sull'intelligenza artificiale. L'esperienza di visione viene ottimizzata attraverso l'iMDP, una piattaforma progettata per garantire la piena *governance* dell'intero processo di *streaming*, un'elevata qualità del servizio e un buon ritorno sull'investimento. Il numero di spettatori *online* al giorno d'oggi è aumentato notevolmente e, di conseguenza, i proprietari di contenuti vogliono garantire una QoE e QoS adeguata agli utenti. L' iMDP è una piattaforma *all-in-one* che garantisce il controllo completo sul processo di *streaming* e la possibilità di raggiungere utenti ovunque, su qualsiasi dispositivo connesso e nel modo più veloce possibile. La piattaforma iMDP è progettata per la distribuzione di video in *streaming*, è una piattaforma singola integrata basata su tecnologie proprietarie AI-Powered. Le sue caratteristiche ottimizzano le risorse, danno grande attenzione al tema della sostenibilità e massimizzano il ritorno sull'investimento, fornendo piena trasparenza e controllo sul processo di *streaming*.

L'iMDP gestisce l'intero processo di creazione e distribuzione dei *media* e assicura:

- La risoluzione dei problemi associati allo *streaming live* su larga scala, mantenendo una qualità video e audio estremamente elevata senza ritardi o interruzioni.
- Una semplice integrazione con l'infrastruttura esistente del cliente.
- La piena visibilità, il controllo e la *governance* sull'intero flusso di lavoro e processo di distribuzione.
- La riduzione al minimo dei consumi energetici e dei costi di gestione.

## **La *Private Network***

Lo *streaming online* ha un impatto significativo sulle reti di distribuzione poiché deve soddisfare alcuni requisiti come scalabilità, qualità e affidabilità. Inoltre, tutti questi problemi devono essere gestiti al minor costo possibile. La *AI Media Delivery* di MainStreaming aumenta l'affidabilità della distribuzione, riduce la latenza e previene la congestione, garantendo la massima qualità dell'esperienza per gli spettatori.

La piattaforma si basa su infrastrutture tecnologiche e reti di proprietà globale concepite esclusivamente per la distribuzione di video in tempo reale. Garantisce inoltre un servizio flessibile che si adatta facilmente a qualsiasi attività commerciale.

### 1. *Global private network* (Rete privata globale)

La piattaforma di distribuzione multimediale intelligente (iMDP) può supportare facilmente qualsiasi tipo di servizio e modello di *business*, indipendentemente dalle dimensioni dell'azienda o dalla sua maturità aziendale. La rete privata globale di MainStreaming è un servizio di distribuzione multimediale *all-inclusive* progettato specificamente per esigenze di distribuzione a basso volume o di punta e offre una *governance* completa sul flusso di lavoro in *streaming*. L'iMDP si fonda su una dorsale di rete privata globale di oltre 4300 interconnessioni con ISP in tutto il mondo, che migliorano le capacità di *streaming* e riducono la latenza, rendendo la soluzione ideale per le aziende regionali e globali che trasmettono contenuti in *streaming* digitale.

### 2. *Dedicated Private Network* (Rete Privata Dedicata)

La piattaforma di distribuzione multimediale intelligente include un'opzione di rete privata dedicata, che distribuisce capacità all'interno delle infrastrutture ISP o tramite *peering*, prendendo in considerazione le posizioni dei vari utenti. Con questa opzione il cliente può godere di una rete dedicata agile e scalabile, che garantisce connettività e sicurezza per la trasmissione di video *online*.

### 3. *Hybrid Private Network* (Rete privata ibrida)

La iMDP *Hybrid Private Network* è un *mix* di soluzioni di reti private dedicate e globali, interconnesse con oltre 4.300 *provider* di servizi Internet. Con questa opzione ibrida, il cliente può aggiungere sedi dedicate in cui ha la necessità di più capacità per servire un vasto pubblico. L'opzione *Hybrid Private Network* massimizza la qualità, la larghezza di banda, la scalabilità e la ridondanza della rete.

## 3.7 Cloudflare

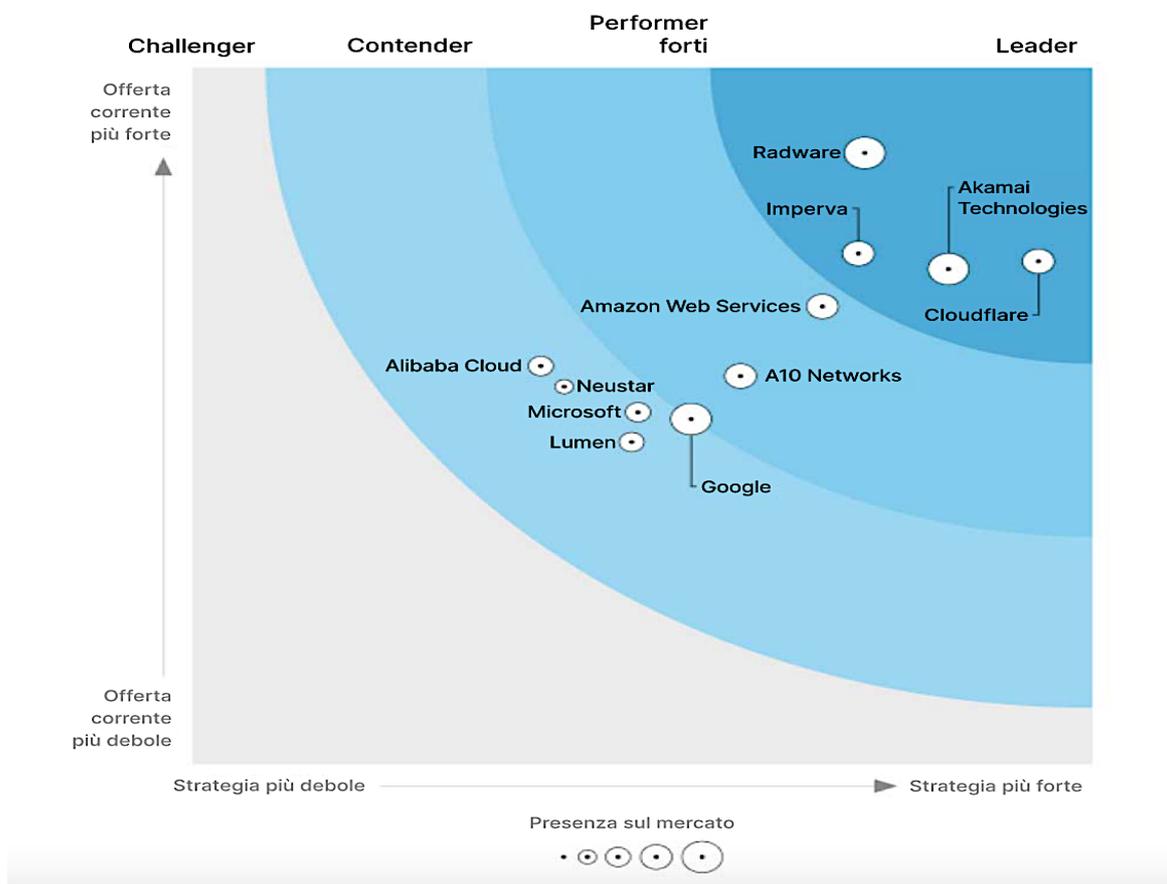
Cloudflare è nata come una semplice applicazione con la funzione di scoprire l'origine della posta indesiderata (SPAM). Con il passare del tempo, l'azienda è cresciuta ed attualmente offre una serie di servizi volti a proteggere i siti *web* da diversi tipi di attacchi, ottimizzandone allo stesso tempo le prestazioni.

È stata creata nel 2009 da Matthew Prince, Lee Holloway e Michelle Zatlyn, che avevano lavorato assieme al progetto *Project Honey Pot*. Cloudflare Inc. è una società americana che si occupa di *content delivery network* (rete per la consegna di contenuti), servizi di sicurezza Internet e servizi di DNS distribuiti, che si pongono tra i visitatori di un sito e gli *hosting provider* degli utenti Cloudflare, agendo come un *reverse proxy server* per siti *web*. L'offerta di Cloudflare si articola su 2 diverse soluzioni:

## 1. Protezione da attacchi DDoS

La protezione da attacchi DDoS di Cloudflare protegge siti *web*, applicazioni e intere reti, garantendo al contempo che le prestazioni del traffico legittimo non vengano compromesse. La rete da 67 Tbps di Cloudflare blocca in media 70 miliardi di minacce al giorno, tra cui alcuni dei più grandi attacchi DDoS della storia. Forrester Research, Inc. ha valutato 11 dei *provider* più importanti nel mercato per la mitigazione DDoS in base a 28 criteri relativi ad offerta corrente, strategia e presenza sul mercato. Nel report di Forrester, Cloudflare è stato nominata ‘Leader’ [Figura 46]<sup>53</sup>. Secondo Forrester, “Cloudflare protegge rapidamente dagli attacchi DDoS già dal perimetro e i clienti vedono la rete perimetrale di Cloudflare come un mezzo convincente per proteggere e fornire applicazioni.” Cloudflare ha inoltre ricevuto i più alti punteggi possibili in 15 diversi settori, tra cui: aree operative di sicurezza, automazione delle risposte, velocità di implementazione, visione del prodotto e prestazioni.

Figura 46 - Soluzioni di mitigazione DDoS, “Forrester Wave”.



Fonte: *The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021*

<sup>53</sup> *The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021*, Forrester.

La protezione da attacchi DDoS illimitata e sempre attiva per le risorse *web* (HTTP/HTTPS) è basata sull'*intelligence* ricavata dalla rete globale di Cloudflare, una rete in continua evoluzione cognitiva. Tale soluzione di protezione lavora in tandem con il *cloud* Web Application Firewall (WAF), il Bot Management e altri servizi di sicurezza L3/4, per proteggere le risorse da minacce informatiche di ogni tipo. Cloudflare Spectrum è un servizio di *proxy* inverso che fornisce protezione da attacchi DDoS per qualsiasi applicazione (non solo *web*), come FTP, SSH, VoIP, *gaming* o qualsiasi applicazione in esecuzione su un protocollo TCP/UDP. Spectrum è dotato di bilanciamento del carico integrato e accelerazione del traffico per il traffico L4. Magic Transit di Cloudflare offre una protezione da attacchi DDoS basata su BGP per l'infrastruttura di rete, a scelta nelle modalità di distribuzione “*always-on*” oppure “*on-demand*”. I *data center* in tutte le 200 città controllano le *subnet* dei clienti per assorbire il traffico di rete e mitigare le minacce vicine alla fonte d'attacco.

## 2. Cloudflare CDN

Cloudflare offre contenuti statici e dinamici tramite la sua rete perimetrale diffusa in tutto il mondo. Esercita un controllo preciso sul modo in cui i contenuti vengono memorizzati nella *cache*, riduce i costi della larghezza di banda e sfrutta la protezione DDoS integrata e senza limiti.

Cloudflare ha realizzato una rete globale estesa di *data center* in grado di memorizzare i contenuti statici in prossimità dei clienti e di fornire i contenuti dinamici sulle dorsali private [Figura 47]. La rete di Cloudflare è del tipo *API-first* e permette ai clienti di automatizzare con facilità i flussi di lavoro e di esercitare un controllo molto preciso sul modo in cui i contenuti vengono memorizzati ed eliminati. Con Cloudflare Workers, i clienti possono personalizzare il *caching* con facilità a seconda delle esigenze delle loro applicazioni. Il *caching* dei contenuti nella rete di Cloudflare riduce al minimo la necessità di estrazione del contenuto dall'origine, riducendo in questo modo i costi. Inoltre, i clienti condivisi con i *partner* di Cloudflare hanno diritto a tariffe sui dati in uscita dal *cloud* sensibilmente scontate, grazie alla *Bandwidth Alliance*.

Cloudflare supporta circa 25 milioni di proprietà Internet ed è in grado di indirizzare in modo intelligente e veloce le richieste di contenuti che arrivano sulla propria rete. Il traffico può inoltre essere ridistribuito su più origini, usando i criteri della vicinanza geografica e della latenza di rete per determinare la destinazione più efficace per ciascuna richiesta. Cloudflare consente di adottare un controllo avanzato sui modi in cui i contenuti vengono memorizzati nella *cache* della propria rete. Page Rules permette di definire un comportamento particolare per singolo URL, tra cui cosa viene memorizzato sulla *cache* e per quanto tempo. L'API *Cache* di Cloudflare permette ai clienti di avere maggiore controllo su come i contenuti vengono memorizzati sulla *cache*, migliorando l'*hit rate* grazie al *routing* avanzato e alla canalizzazione dell'URL.

Il *caching* dei contenuti nella rete Cloudflare riduce il numero di richieste indirizzate a un'origine grazie all'estrazione di contenuti statici da un *datacenter* Cloudflare, riducendo al minimo il consumo di banda. Cloudflare propone tariffe trasparenti per la larghezza di banda, senza aumenti in caso di attacchi. I clienti che si appoggiano a *partner* di Cloudflare per l'*hosting* dei propri siti *web* possono ridurre o eliminare interamente gli addebiti per i dati in uscita dai propri *provider* di *hosting* verso Cloudflare, in caso di richieste di contenuti dinamici.

Figura 47 - Funzionamento della CDN di CloudFlare.



Fonte: *Cloudflare.com*

Cloudflare offre un insieme di soluzioni adatte per i video, attraverso un ecosistema di prestazioni e servizi di sicurezza tarati appositamente per i contenuti video. La rete Anycast globale di Cloudflare garantisce una diffusione video veloce, con tempi più brevi di avvio dei filmati e *buffering* ridotto, ovunque siano ubicati i visitatori. Funzionalità quali *Concurrent Streaming Acceleration* ottimizzano ancora di più l'offerta di video in diretta, anche in presenza di una serie di richieste in simultanea e con latenza *end-to-end* minima.

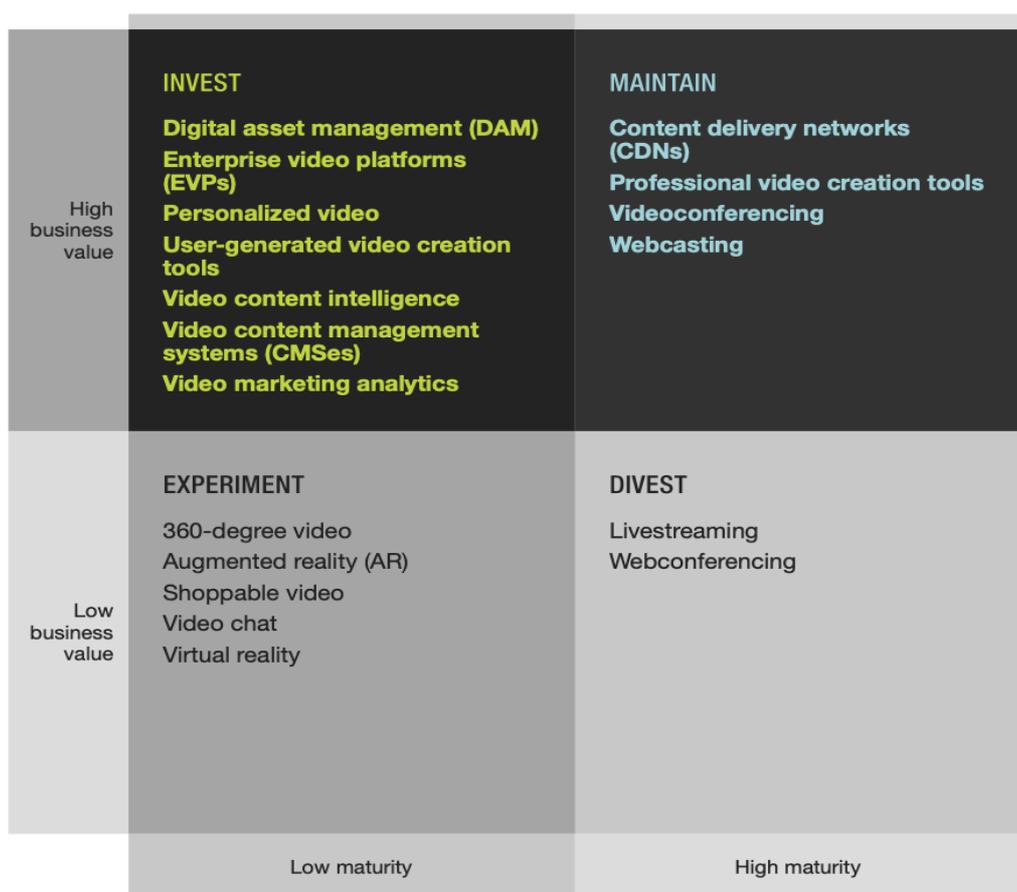


# CONCLUSIONI

Mentre molti desiderano che il biennio 2020-2021 sia presto dimenticato, per lo *streaming* sarà ricordato come un periodo di svolta. L'industria ha fornito nuovi servizi, lo *streaming* ha fatto registrare incredibili picchi di crescita, i *blockbuster* sono stati rilasciati direttamente in *streaming* e i *social media* occupano una posizione sempre più centrale nella vita e nelle abitudini delle persone. Il 2020-2021 è stato caratterizzato dalla volatilità e l'industria dello *streaming* non è stata esentata. La transizione globale allo *streaming* è tutt'altro che completa in quanto non satura. Sia i mercati in cui lo *streaming* è consolidato (America, Asia), sia quelli in cui ancora non lo è (Africa, Sud America) fanno registrare una crescita costante nel tempo di visualizzazione<sup>54</sup>. La somma di tutte le forme di IP video, che include Internet Video, IP VOD, *file* video scambiati via *file sharing*, servizi di videoconferenza e video *streaming* in ambito *gaming*, conterà tra l'80% e il 90% dell'intero traffico IP, arrivando all'82% entro il 2022.

Ma per far prosperare l'industria, tali tendenze devono continuare: il principale rischio è il cosiddetto “*streaming burnout*” legato al comportamento dei consumatori che cercano attività fuori casa.

Figura 48 - Tecnologie video per l'esperienza di clienti e dipendenti.



Fonte: The Forrester Tech Tide

<sup>54</sup> Conviva's State of Streaming, Conviva, 2020.

Come sostenuto dal rapporto di Forrester<sup>55</sup>, che analizza la maturità ed il valore del *business* per 18 differenti tecnologie riguardanti il video, le CDN rientrano nel quadrante *Maintain* caratterizzato da elevata maturità ed alto valore aziendale [Figura 48]. Questa tecnologia è presente sul mercato da decenni e il nucleo di funzionalità è rimasto sostanzialmente invariato. Le CDN sono e saranno essenziali per offrire un'esperienza di *streaming* video di alta qualità. Gran parte del traffico Internet viene gestito tramite CDN e, nello specifico, entro il 2022, il 72% del traffico sarà trasportato tramite CDN, con un aumento significativo dal 56% del 2017. La quota di traffico gestita ai bordi della rete (*EDGE*) è quindi destinata ad aumentare progressivamente. Data la rilevanza, la centralità ed il valore delle CDN, si registreranno tentativi di entrata da parte di nuovi operatori e vi sarà una competizione molto forte all'interno del mercato, sia per quanto riguarda il prezzo che per la conquista di quote di mercato. Si tratta di un *business* in cui non sono presenti dinamiche concorrenziali come, ad esempio, nel contesto dei *social media*, nel quale l'arrivo di Tik Tok potrebbe corrispondere all'uscita dal mercato di Snapchat o Instagram. Gli *asset* di capitale, come ad esempio i *server* poggiati nei vari POP degli operatori telefonici a livello mondiale, sono il traguardo di vent'anni di progressione dell'architettura, caratterizzata da investimenti, sviluppo e crescita dell'infrastruttura. Un vantaggio competitivo acquisito in termini di *asset* (rete, *server*, infrastrutture) è difficilmente *displaceable*. In tale contesto è quindi presente una rendita di posizione molto forte derivante dagli investimenti storici e incrementali. Infatti, se un *player* come Mainstreaming volesse offrire le stesse capacità di Akamai in Italia, dovrebbe sostenere un investimento molto elevato rispetto alle proprie possibilità economiche. Sono quindi presenti elevate barriere all'ingresso, sia dal punto di vista finanziario che dal punto di vista del *know-how*.

Tra i tre livelli di concorrenza e competizione precedentemente analizzati, le principali insidie per gli operatori di CDN già presenti nel mercato provengono dai *Big Tech*, come Amazon e Google. Infatti, queste realtà sono considerate delle aziende-stato date le loro dimensioni, i loro volumi e il fatturato, che ammonta a 386 miliardi per Amazon e 183 miliardi per Google. Dati questi numeri è evidente che nel momento in cui le *Big Tech* vogliono presidiare integralmente il mercato del *content delivery*, hanno le capacità di investimento per farlo, sostituendo Akamai (3,2 miliardi di fatturato), principale *player* nel mercato delle CDN, e, a maggior ragione, i *player* minori come Limelight e Fastly. La posizione di Akamai sembra quindi difficilmente attaccabile dagli operatori presenti nel livello 2 e 3 della *competition*, mentre risulta attaccabile dai *Big Tech*, qualora ritengano necessario per la loro strategia competitiva presidiare il mercato delle CDN.

---

<sup>55</sup> *The Forrester Tech Tide: Video Technologies For Customer And Employee Experience*, FORRESTER, 2019.



# APPENDICE SULLA SICUREZZA

## 1. Tipologie di attacchi

Nel 2020 il traffico Internet ha registrato una forte crescita e i criminali hanno approfittato di questa situazione, impiegando il tempo passato forzatamente a casa per modificare per sempre il panorama delle minacce. Si è verificato un forte aumento negli attacchi di *credential stuffing*, alle applicazioni *web*, DDoS e di *phishing*.

- *Credential Stuffing*: si tratta di un attacco che fa leva sulla probabilità che le persone possano utilizzare lo stesso nome utente e la stessa *password* per accedere a più applicazioni, siti e servizi. I cybercriminali acquisiscono i dettagli degli *account* rubati da una piattaforma e implementano i *bot* necessari per accedere a molti altri *account* con le stesse credenziali. Una volta trovato il modo di accedere, i criminali violano *l'account*, effettuando acquisti fraudolenti o sottraendo informazioni riservate, fino a quando il relativo proprietario non se ne accorgerà<sup>56</sup>.
- Applicazioni *web*: gli attacchi a livello di applicazione sono una minaccia sempre più comune alla sicurezza sul *web*. Questo tipo di attacchi si serve di numerosi mezzi per indebolire e penetrare all'interno di un sito *web*, provocando una diminuzione delle prestazioni dei siti, violazioni di dati e un'esposizione dell'infrastruttura. Gli attacchi a livello di applicazione possono essere diretti contro diversi tipi di funzionalità all'interno di un sito. Possono essere rivolti direttamente contro l'applicazione *web* oppure essere inoltrati a un *database* dove vengono compromesse le informazioni archiviate al suo interno.

Che vengano archiviate informazioni sensibili su un sito *web*, o che un determinato sito *web* funzioni unicamente come sito promozionale, gli attacchi alle applicazioni *web* possono avere un impatto negativo sia sulle prestazioni aziendali sia sul marchio in generale.

Tre sono i principali tipi di attacco:

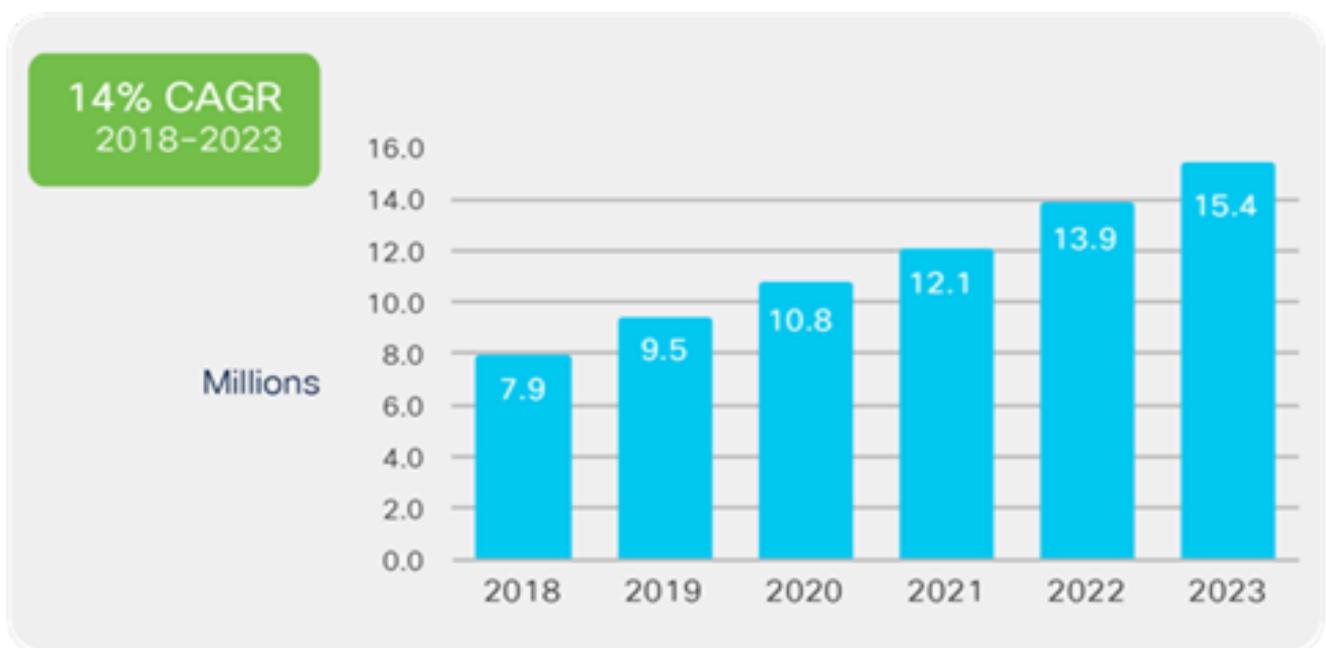
1. L'attacco SQL Injection, nell'ambito del quale delle false *query* di *database* vengono usate per destabilizzare o infiltrare applicazioni e *database* critici.
2. L'attacco XSS (*Cross Site Scripting*), in cui le vulnerabilità nello *scripting* XSS permettono ai criminali di inserire uno *script* che viene poi eseguito nel *browser* dell'utente.

---

<sup>56</sup> *Credential stuffing cos'è? Ecco gli effetti di questa tipologia di attacchi*, 7 giugno 2019, Articolo pubblicato su: NetworkDigital360.

3. L'attacco MFE (*Malicious File Execution*), tramite il quale gli *hacker* sono in grado di inserire dati ostili e di codificarli sfruttando una vulnerabilità dell'applicazione agli attacchi RFI (*Remote File Inclusion*).
- DDoS: Un attacco *Distributed Denial-of-Service*, comunemente noto come attacco DDoS, consiste nel tentativo di sovraccaricare un sito *web* o un servizio *online* con traffico proveniente da diverse origini in modo da renderlo non disponibile agli utenti. Poiché le organizzazioni trasferiscono *online* sempre più dati e processi aziendali, la scalabilità e la frequenza degli attacchi *Denial of Service* continuano ad aumentare [Grafico 49]. Per difendersi dagli attacchi DDoS, le organizzazioni hanno bisogno di una protezione semplice, rapida ed efficace in grado di tutelare la presenza *web*, il *brand* e i ricavi.

Grafico 49 - Il numero di attacchi DDoS a livello globale raggiungeranno i 15,4 milioni entro il 2023.



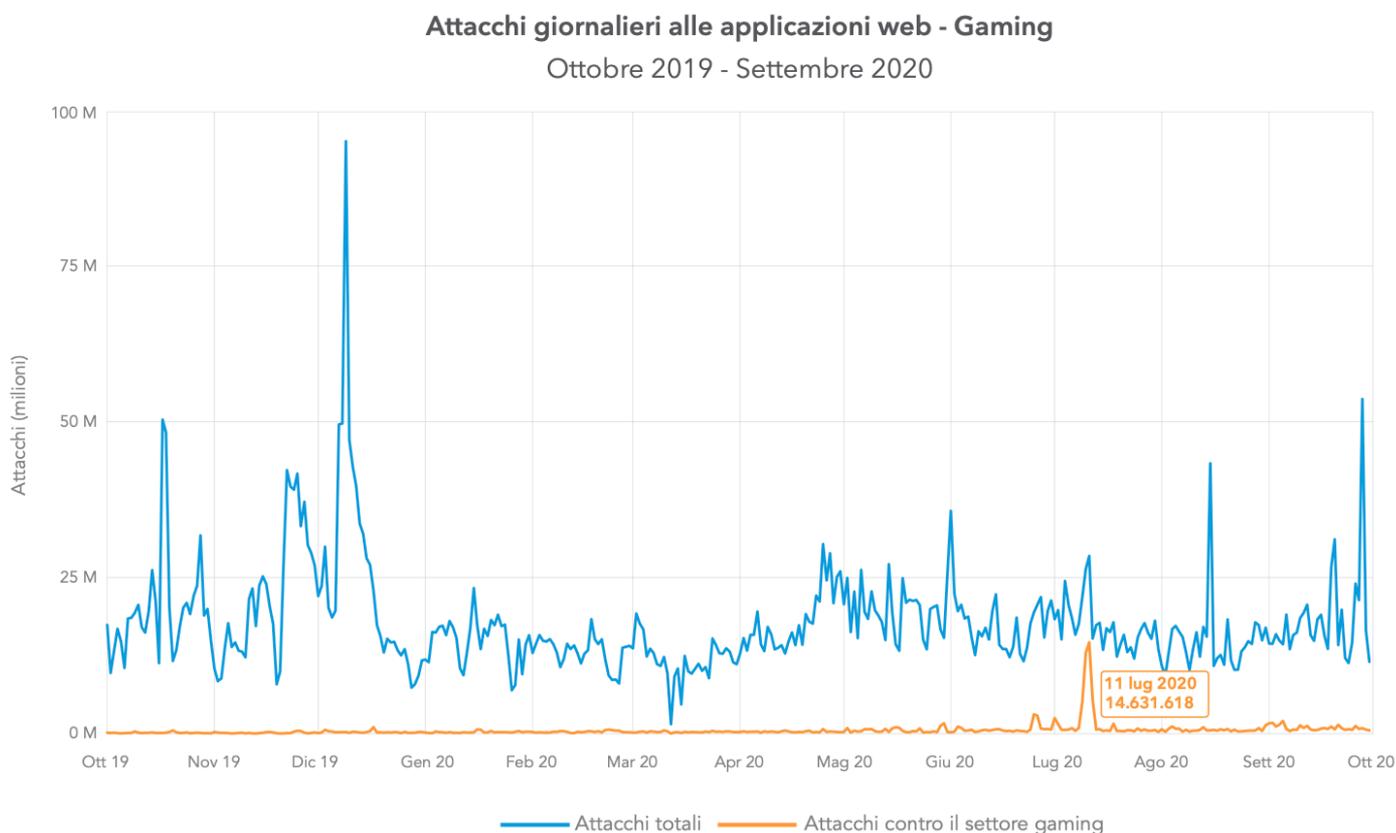
Fonte: Cisco Visual Networking Index™ (Cisco VNITM)

- *Phishing*: il *phishing* è l'atto con il quale si tenta di ingannare il destinatario di un messaggio *e-mail* dannoso, facendo sì che lo apra e ne esegua le istruzioni. Il "mittente" del messaggio inganna la vittima facendole credere che l'*e-mail* sia stata inviata da una fonte affidabile, come un ufficio governativo, un fornitore o un cliente dell'azienda. L'*e-mail* di *phishing* può includere un allegato dannoso, come un documento PDF o Word, che, una volta aperto, danneggerà il computer dell'utente mediante l'installazione di *malware*. Oppure l'*e-mail phishing* può contenere nel testo un *link* a un URL dannoso. Quando l'utente fa *clic* su questo *link*, potrebbe essere indirizzato a un sito apparentemente legittimo, ma che in realtà è utilizzato per raccogliere informazioni riservate quali nomi utente e *password* o per installare *malware* sul dispositivo.

Diversi sono i settori in cui la sicurezza della rete è diventata ormai un tema centrale e verso la quale è necessario adottare delle contromisure. Ad esempio, i settori *retail*, *hospitality* e viaggi hanno attratto un sorprendente 63% di attacchi di *credential stuffing* e un 41% di attacchi *web*.

Il *gaming* ha registrato la maggior crescita nel numero di attacchi rispetto a tutti gli altri settori nel 2020. Gli attacchi *web* rivolti al settore del *gaming* sono aumentati del 340% tra il 2019 e il 2020 [Grafico 50] e gli attacchi di *credential stuffing* sono aumentati del 224%. Stranamente, gli attacchi DDoS sferrati contro il settore del *gaming* sono diminuiti di quasi il 20% nello stesso periodo<sup>57</sup>. È proprio per tale tendenza che vari *player* nel mercato delle CDN come Akamai e AWS pongono sempre più attenzione sull'offerta di servizi di qualità per quanto riguarda la sicurezza.

Grafico 50 - Attacchi giornalieri alle applicazioni web – Gaming.



Fonte: Rapporto sullo stato di Internet 2020, Security, AKAMAI, 2020

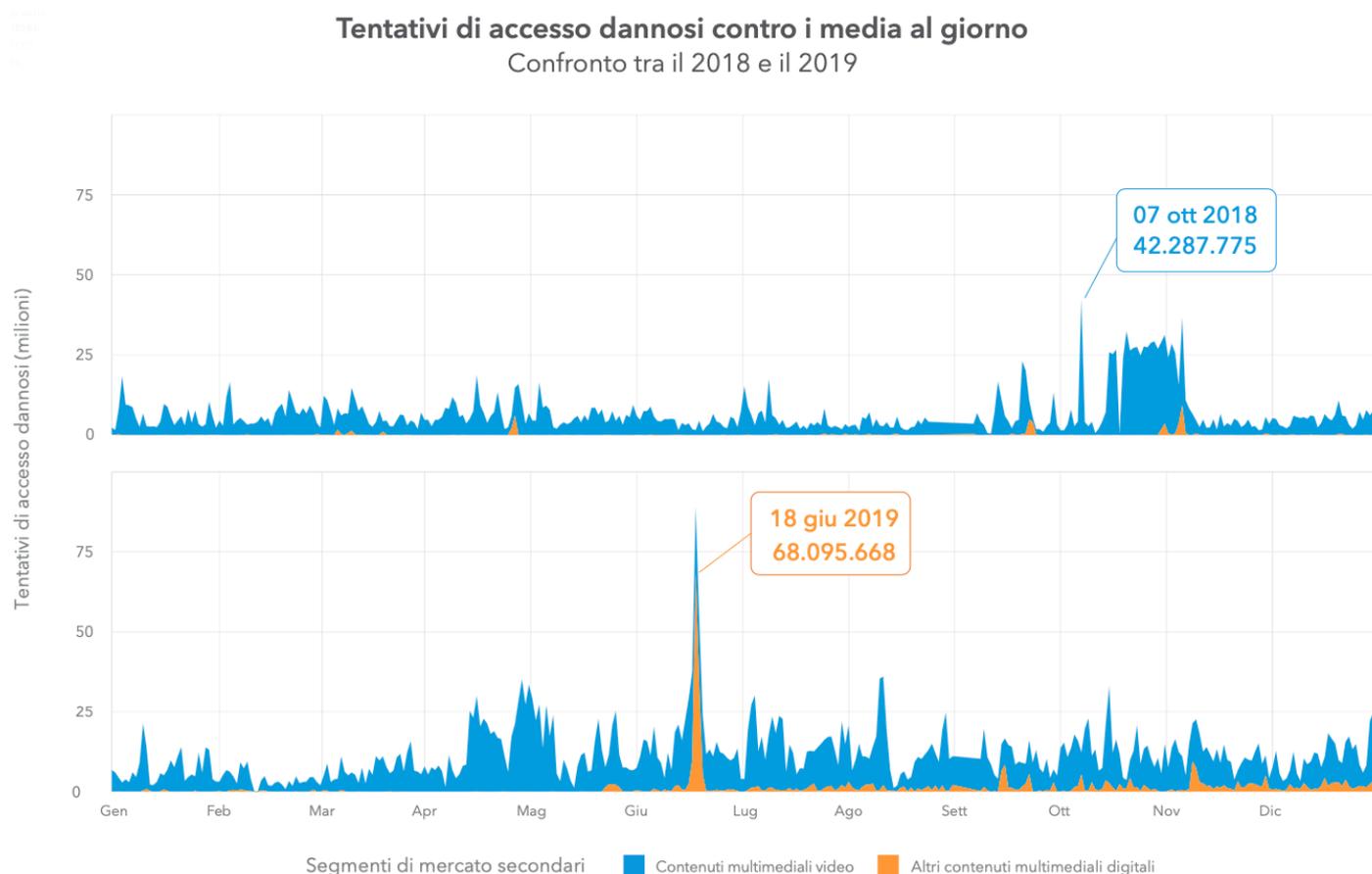
A causa del Covid-19 Alcune tendenze degli attacchi sono continuate e molte sono cresciute in modo esponenziale. Nel 2019, l'aumento del 208% negli attacchi di *credential stuffing* contro i siti *web* di video è passato in secondo piano rispetto all'incremento del 1.450% nel primo trimestre 2020.

<sup>57</sup> Rapporto sullo stato di Internet 2020, Security, AKAMAI, 2020.

## 2. Il settore *media*

Secondo il rapporto di Akamai, il settore dei *media* ha subito 17 miliardi di attacchi di *credential stuffing* tra gennaio 2018 e dicembre 2019 [Grafico 51] ed è stato rilevato che il 20% degli 88 miliardi di attacchi di *credential stuffing* totali osservati durante il periodo di riferimento hanno preso di mira le società di *media*<sup>58</sup>.

Grafico 51 - Tentativi di accesso dannosi contro i *media* al giorno.



- Si è registrato un flusso costante di attacchi di *credential stuffing* sferrati contro il settore dei *media* negli ultimi 24 mesi

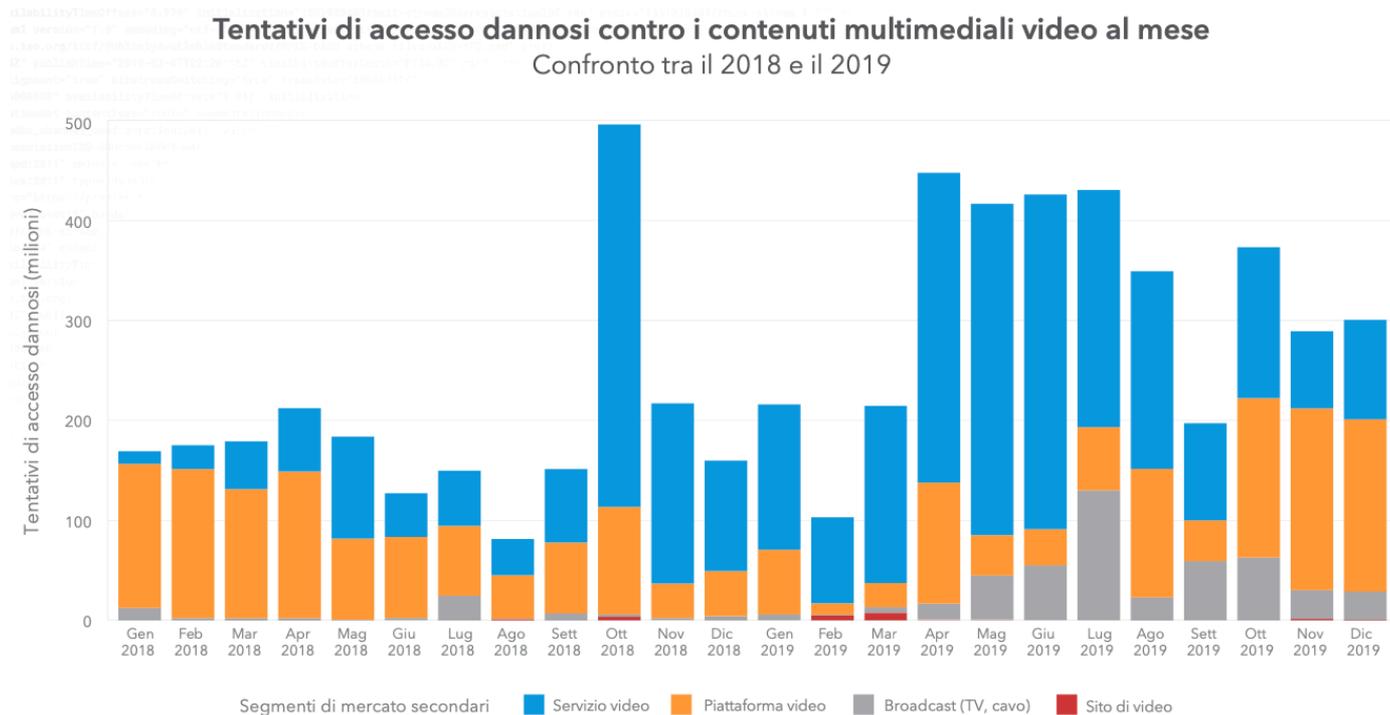
Fonte: *Rapporto sullo Stato di Internet 2020, Security: Media, Akamai, 2020*

Le società dei *media* rappresentano un obiettivo attraente per i criminali, infatti si è registrato un aumento degli attacchi nel settore dei *media video* anno dopo anno del 63%. Il rapporto mostra anche un aumento del 630% e del 208% su base annua degli attacchi contro TV e siti di video, rispettivamente. Allo stesso tempo, gli attacchi contro i servizi video sono aumentati del 98%, mentre quelli contro le piattaforme video sono diminuiti del 5% [Grafico 52]. Il marcato aumento degli attacchi rivolti alla TV e ai siti di video sembra coincidere con un'esplosione nel 2019 dei contenuti multimediali *on-demand*. Secondo Steve Ragan,

<sup>58</sup> *Rapporto sullo Stato di Internet 2020, Security: Media, AKAMAI, 2020.*

ricercatore sulla sicurezza di Akamai e autore del rapporto sullo stato di Internet con *focus* sulla sicurezza, gran parte del valore degli *account* del settore dei *media* risiede nel potenziale accesso sia alle risorse compromesse, come i contenuti *premium*, sia ai dati personali. "Abbiamo osservato una tendenza in cui i criminali combinano le credenziali di un *account* multimediale con l'accesso a punti premio rubati dai ristoranti locali e commercializzano l'offerta come pacchetti *'date night'*", ha spiegato Ragan nel rapporto. "Una volta che i criminali ottengono le informazioni sulla posizione geografica degli *account* compromessi, possono abbinarle per essere vendute come una cena e un film".

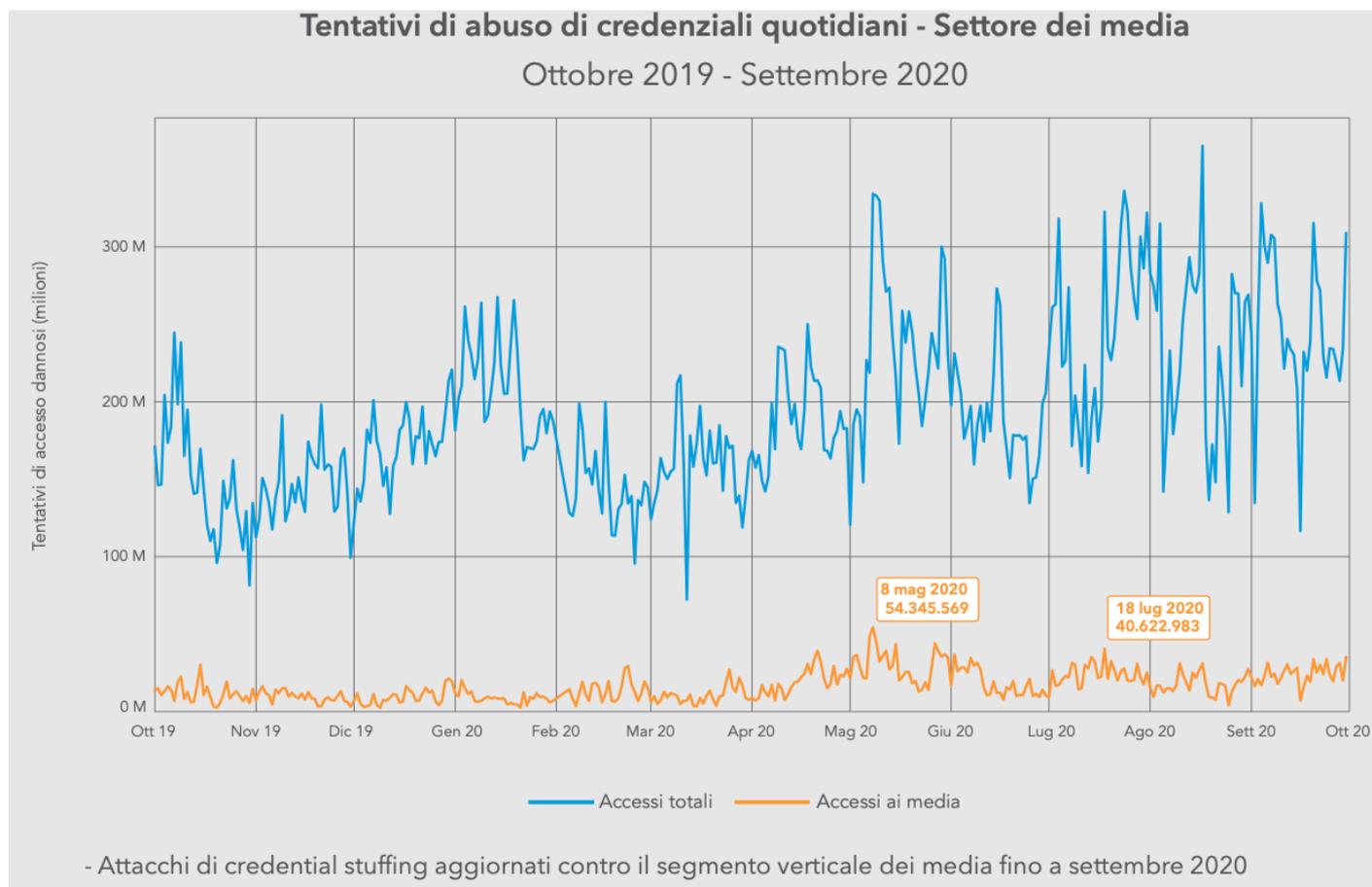
Grafico 52 - Tentativi di accesso dannosi contro i contenuti multimediali video al mese.



Fonte: Rapporto sullo Stato di Internet 2020, Security: Media, Akamai, 2020

Tuttavia, i siti di video non sono l'unico obiettivo degli attacchi di *credential stuffing* nel settore dei *media*. Infatti, si registra un incredibile aumento del 7.000% degli attacchi mirati ai contenuti pubblicati *online*, come giornali, libri e riviste, che sono nel mirino dei criminali informatici.

Gli Stati Uniti sono stati di gran lunga la principale fonte di attacchi di *credential stuffing* contro le società di *media* con 1,1 miliardi nel 2019, con un aumento del 162% rispetto al 2018. Francia e Russia sono state rispettivamente la seconda e la terza con 3,9 milioni e 2,4 milioni di attacchi. L'India è stato il paese più preso di mira nel 2019, resistendo a 2,4 miliardi di attacchi di riempimento delle credenziali. Seguono gli Stati Uniti con 1,4 miliardi e il Regno Unito con 124 milioni.



Fonte: Rapporto sullo Stato di Internet 2020, Security: Media, Akamai, 2020

### 3. Aggiornamento q1 2020

A causa dell'avvento della pandemia di Covid-19 si è verificato un forte picco di tentativi di accesso dannosi contro fornitori di servizi video ed emittenti europei durante il primo trimestre del 2020. Un attacco a fine marzo, dopo l'istituzione di molti protocolli di isolamento, ha diretto quasi 350.000.000 di tentativi contro un singolo fornitore per un periodo di 24 ore.

Un'altra tendenza rilevante emersa durante il primo trimestre è stata il numero di criminali che hanno condiviso l'accesso gratuito ai giornali, spesso offerti come veicoli di autopromozione. Inoltre, si è osservato una diminuzione nel costo delle credenziali degli *account* rubate nel corso del trimestre, che inizialmente è stato scambiato per una cifra compresa tra \$1 e \$5 e tra i \$10 a \$45 per le offerte di pacchetti composti da vari servizi. Questi prezzi sono diminuiti quando nuovi *account* e liste di credenziali riciclate hanno popolato il mercato.

Grafico 54 - Tentativi di accesso dannosi contro i media al giorno.

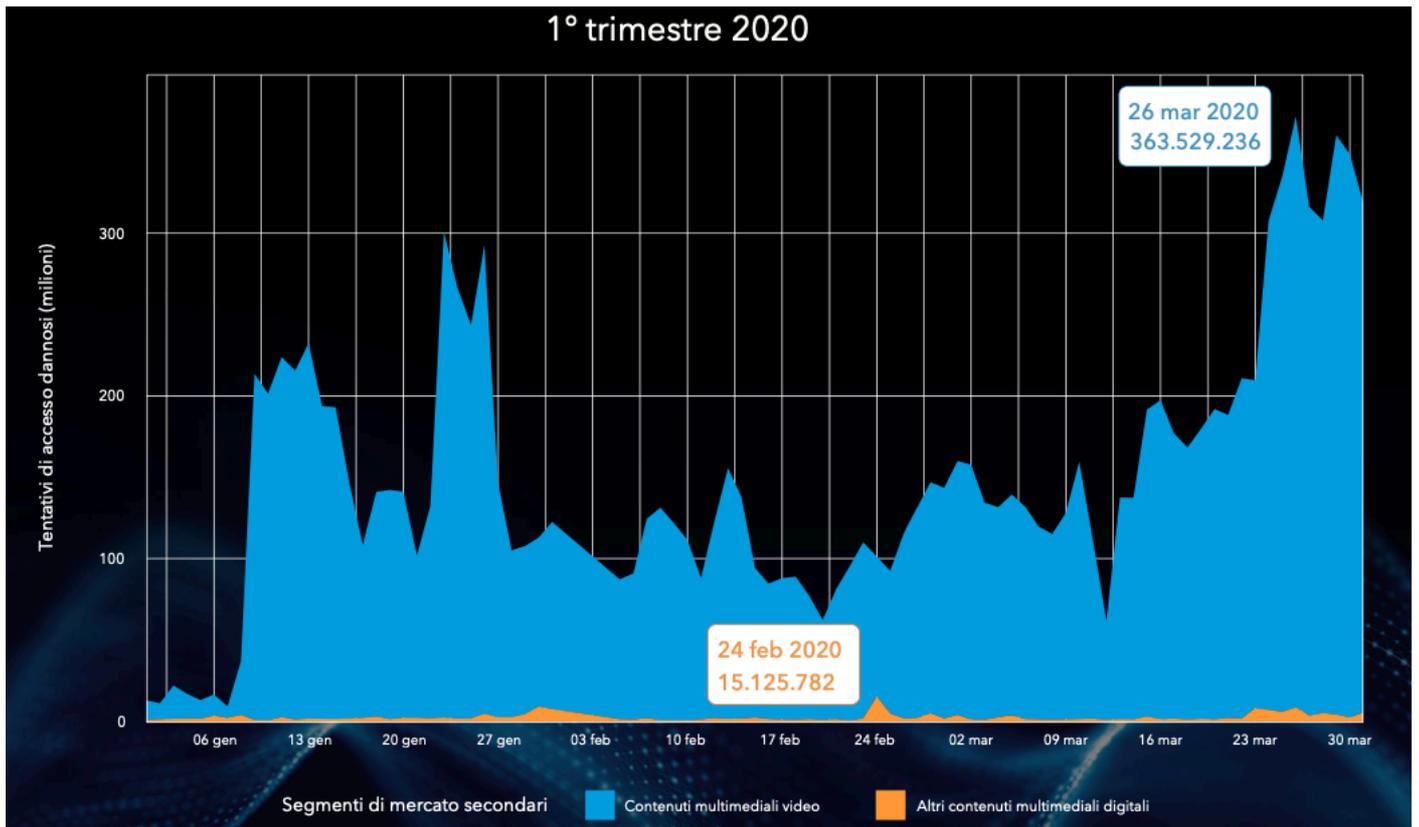


Grafico 55 - Tentativi di accesso dannosi contro i contenuti multimediali video al mese.

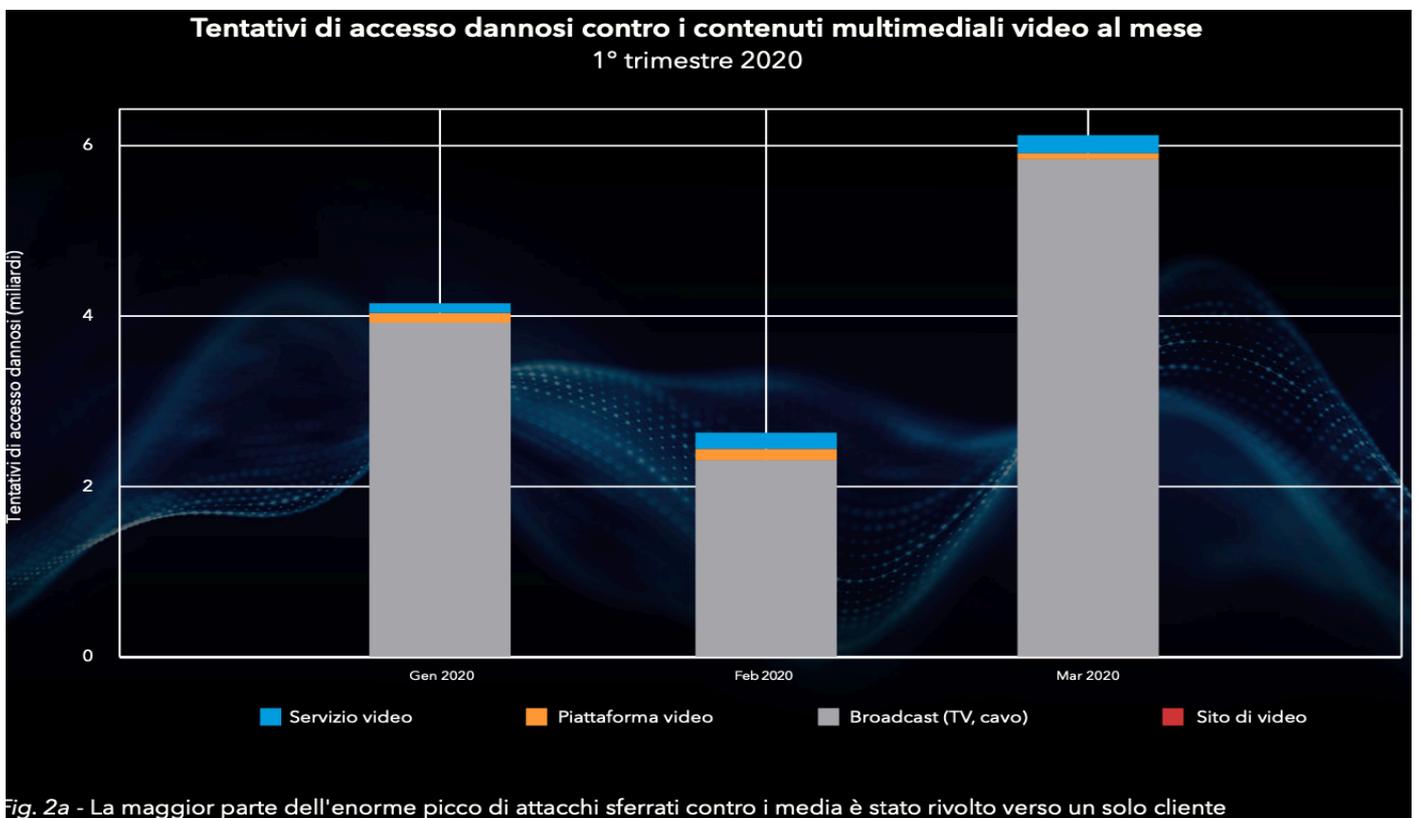


Fig. 2a - La maggior parte dell'enorme picco di attacchi sferrati contro i media è stato rivolto verso un solo cliente

Non si rimarca mai troppo l'enorme impatto sia attuale che potenziale esercitato dagli attacchi di *credential stuffing* sulle aziende. Finché esisteranno nomi utente e *password*, i criminali cercheranno di prenderli di mira, mettendo a rischio consumatori, organizzazioni e le loro preziose informazioni.

Il riciclaggio e la condivisione delle *password* rappresentano i fattori che contribuiscono maggiormente in tal senso: ecco perché sono così importanti i programmi di sensibilizzazione che spiegano i rischi correlati con queste pratiche. Inoltre, si avverte la forte esigenza di adottare metodi di autenticazione più solidi, come l'autenticazione multifattore, che protegge ulteriormente gli *account* dagli attacchi.

L'economia criminale è costituita da eventi concatenati, in cui tutte le parti sono tra loro collegate e tutte le informazioni sono preziose. I criminali preparano i loro *account* compromessi e li vendono in base a caratteristiche di interesse, area geografica e volume, rivolgendosi a persone intenzionate a pagare, il che va solo ad alimentare le loro azioni illegali, mantenendoli sempre più focalizzati sul modo con cui poter eludere i sistemi di rilevamento e mitigazione degli attacchi. Ecco perché i responsabili aziendali e i *team* addetti alla sicurezza investono notevolmente in termini di tempo ed energia nell'intento di sviluppare nuovi sistemi di difesa e protezione.

Non esiste tuttavia una ricetta magica. La lotta contro il *credential stuffing* richiede investimenti ingenti in strumenti tecnologici, persone e lo sviluppo di *policy* intelligenti per proteggere le risorse senza influire sugli utenti finali: nel caso del settore *media*, chi cerca di guardare il proprio programma televisivo o evento sportivo preferito comodamente a casa sua.

## RINGRAZIAMENTI

Desidero esprimere il mio sincero ringraziamento a tutti coloro che hanno contribuito a rendere possibile questa tappa fondamentale dei miei studi e della mia vita.

Ringrazio innanzitutto il Prof. Luca Balestrieri, relatore di questa tesi di laurea, per la grande competenza, l'attenta guida e la generosa disponibilità dimostrata durante lo sviluppo della tesi.

Un ringraziamento speciale all'Ing. Daniele Alberto Rascio per l'attenzione, la puntualità, l'aiuto nel reperimento di informazioni e contenuti fondamentali per l'elaborato e per il tempo dedicato a correggere le diverse bozze.

Con questo scritto concludo un grande capitolo della mia vita e contemporaneamente ne apro uno nuovo. Mi è chiaro che niente di tutto ciò sarebbe stato possibile senza avere al mio fianco persone che mi hanno sostenuto. Verso di loro ho un grande senso di gratitudine.

Un ringraziamento speciale e profondo va ai miei genitori, Marco e Donatella, senza i quali tutto ciò non sarebbe stato possibile. Grazie per aver assecondato e capito le mie ambizioni, per non avermi mai fatto mancare nulla, per avermi insegnato a non mollare mai e per avermi cresciuto con amore e cura infinita. Siete la mia vita.

Ringrazio mia sorella Agnese e Giovanni per le critiche verso il mio elaborato, per essere continua fonte d'ispirazione e per avermi sostenuto in questo percorso. Grazie nonna Eda. Grazie alla mia splendida famiglia!

Ringrazio tutti i miei amici di una vita, grazie per essere stati presenti anche durante questa ultima fase del mio percorso di studi. Grazie per aver ascoltato i miei sfoghi e grazie per tutti i momenti di spensieratezza e divertimento. Siete nel mio cuore. Una menzione particolare per Simone e Lorenzo che hanno condiviso con me questo breve viaggio di due anni, grazie di avermi sopportato, di aver condiviso lunghe giornate prima a Roma e poi su Teams. Vi voglio bene.

Grazie a te, Gioia, che sei entrata nella mia vita quando questo viaggio era già iniziato. Grazie per essere stata al mio fianco, so che non è facile. Grazie per tutto il tempo che mi hai dedicato.

A tutti voi, grazie di cuore.

## BIBLIOGRAFIA E SITOGRAFIA

*5G e il futuro delle telecomunicazioni*, ERITEL.

*5G La rete di domani, notiziario tecnico*, Gruppo Tim, 2017.

*5G & MULTIMEDIA, notiziario tecnico*, Gruppo Tim, 2017.

*5G: no FTTH, no party: ecco perché la fibra fino a casa è l'infrastruttura definitiva*, CORCOM, 17 aprile 2018. Articolo pubblicato su: [corrierecomunicazioni.it](http://corrierecomunicazioni.it).

*Akamai Annual Report 2019*, Akamai, 2019.

*Akamai Annual Report 2020*, Akamai, 2020.

*Akamai's Edge (A) e Akamai Technologies*, Harvard Business Review.

*Akamai: nel 2020 esplosione di streaming e gaming. Una partita di calcio in streaming genera 1 terabit/s di traffico*, DDAY, 8 febbraio 2021. Articolo pubblicato su Digital Day.

*Akamai Proxy Statement 2019*, Akamai 2019.

*Akamai Proxy Statement 2020*, Akamai 2020.

*Allegato (6 e 7) alla relazione annuale*, AGCOM, 2020.

*Amazon Annual Report 2020*, Amazon, 2020.

*Amazon: il bilancio del 2020*, 19 aprile 2021, Starting Finance.

*Amazon Proxy Statement 2020*, Amazon, 2020.

*Amazon Proxy statement 2021*, Amazon, 2021.

*Amazon in volata: revenue a +21% e il cloud di Aws balza del 34%*, CORCOM, 31 gennaio 2020. Articolo pubblicato su: [corrierecomunicazioni.it](http://corrierecomunicazioni.it).

*Amazon CloudFront for Media: Best Practices for Streaming Media Delivery*, novembre 2020, white paper, Amazon.

*Banda ultralarga, in Italia le linee a 100 Mega superano il 50%*, CORCOM, 23 aprile 2021. Articolo pubblicato su: [corrierecomunicazioni.it](http://corrierecomunicazioni.it).

Bellino Massimiliano, *L'edge computing in ambiente IoT, tutti i vantaggi*, 10 giugno 2020. Articolo pubblicato su: [NetworkDigital360](http://NetworkDigital360).

*Boom dell'e-commerce, il record è italiano: nel 2021 crescita a quota 78%*, CORCOM, 16 aprile 2021. Report pubblicato su: [corrierecomunicazioni.it](http://corrierecomunicazioni.it).

*Breve storia delle CDN*, blog, CRITICALCASE.

*Building the Gigabit Society: An Inclusive Path Toward Its Realization*, November 2016, Boston Consulting Group (BCG).

Calzetta Giancarlo, *Il futuro del Content Delivery passa dalle piattaforme Edge*, 14 dicembre 2019. Articolo pubblicato su: B2BLABS.

*Content Delivery Network, ecco che cos'è e quando usarlo*, 17 dicembre 2018. Articolo pubblicato su: NetworkDigital360.

*Che cos'è una CDN?*, Akamai.

*Cisco annual internet report, 2017-2022*, Cisco, 2019.

*Cisco annual internet report, 2018-2023*, Cisco, 2020.

*Cisco security report 2020*, Cisco, 2020.

*Cisco Visual Networking Index™ (Cisco VNITM)*, Cisco.

*Communications in 2020*, AGCOM, 2020.

*Communication markets monitoring system, COVID-19 monitoring, no. 2/2020*, AGCOM.

*Content Delivery for an Evolving Internet: Choosing the Right CDN for Today & Tomorrow*, white paper, Akamai.

*Conviva's State of Streaming*, Conviva, 2020.

*Coronavirus, raddoppia il traffico internet, boom di connessioni al Nord*, 12 marzo 2020, Il Sole 24 Ore.

*Credential stuffing cos'è? Ecco gli effetti di questa tipologia di attacchi*, 7 giugno 2019, Articolo pubblicato su: NetworkDigital360.

Dini Antonio, *L'avventurosa storia delle CDN*, 3 maggio 2016. Articolo pubblicato su: LINK.

*Distribuzione di contenuti per una rete Internet in continua evoluzione, la CDN giusta per le esigenze di oggi e di domani*, white paper, Akamai.

*Edge computing: cos'è, come implementarlo e quali vantaggi per le imprese*, 18 novembre 2019. Articolo pubblicato su: NetworkDigital360.

*Edge Computing: 5G's secret weapon*, white paper, Juniper Research.

*Edge computing: l'elaborazione ai margini della rete*, 5 dicembre 2019. Articolo pubblicato su: IONOS.

*Entertainment & Media Outlook in Italy 2019-2023*, PWC, 2019.

*Evoluzione della rete ICT*, rivista dell'AEIT, luglio/agosto 2019.

Frollà Andrea, *Reti, tecnologia e contenuti: ecco le sfide della nuova Rai*, 10 maggio 2016. Articolo pubblicato su: NetworkDigital360.

*Full international DESI final study report*, Desi 2020. Report pubblicato su: European Commission.

Gazzè Sebastiano, *Selezione di Percorsi basata su Consenso Asincrono e Distribuito in Edge Computing tramite Database a Grafo*, tesi di laurea magistrale in ingegneria informatica, POLITO, 2017.

*Global consumer trends. COVID-19 edition. The new normal*, Dynata, 2020.

*Il VoD in Europa 2015-2018*, Rapporto di ITMedia Consulting.

*La migliore regolazione per lo sviluppo della gigabit society. Tecnologie abilitanti, evoluzione dei servizi e best option infrastrutturali*, marzo 2018, ITmedia consulting e LUISS dream.

Lelah Manz, *Spostamento sull'edge - una panoramica in una nuova era del computing*, 15 ottobre 2020, Akamai, 2020.

*L'impatto del coronavirus nei settori regolati*, AGCOM, 2020.

*Lo stato di internet, focus sulla security*, Akamai, 2020.

*Making the Internet Business-Ready*, Akamai.

*Magic Quadrant for Cloud Infrastructure and Platform Services*, 27 luglio 2021, GARTNER.

*Media industry embraces streaming transformation*, KPMG, 2020.

*Millenials, 1 milione in più davanti alla tv con il lockdown*, Ansa, 20 aprile 2020.  
Articolo pubblicato su: [ansa.it](https://www.ansa.it).

*Multi-access Edge Computing: la spinta giusta per il 5G?*, 22 gennaio 2021.  
Articolo pubblicato su: [ImpresaCity](https://www.impresacity.com).

*Nuovi modelli di interconnessione IP*, notiziario tecnico, Gruppo Tim.

*Osservatorio sulle piattaforme online*, AGCOM, 2019.

Parada Guiomar, *Industry 4.0 – 2021 – IoT, edge computing and telematic systems with 5G in off-highways vehicles' explosive year*, Il Sole 24 Ore, 5 Gennaio 2021. Articolo pubblicato su: [nova.ilsole24ore.com](https://www.nova.ilsole24ore.com)

*Peer-Assisted Content Distribution in Akamai NetSession*, technical publication, Akamai-Duke-University of Pennsylvania.

*Reti e servizi 5G: accelerazione o frenata?*, 3 aprile 2020, Articolo pubblicato su: [ImpresaCity](https://www.impresacity.com).

*Relazione annuale*, AGCOM, 2020.

*Il 2021 sarà un anno d'oro per lo streaming live. Ma anche per il cybercrime*, 18 gennaio 2021. Articolo pubblicato su: [NetworkDigital360](https://www.networkdigital360.com).

*Rapporto sullo stato di Internet 2020*, Security, AKAMAI, 2020.

*Report on European Analysis 2020*, Desi (Digital Economy and Society Index), 2020.

*Reti di telecomunicazioni e Covid-19. Così le infrastrutture italiane hanno retto all'onda d'urto del lockdown*, 20 novembre 2020, Istituto per la Competitività.

Saporiti Riccardo, *Quanti sono 4,8 zettabyte? Il traffico dati su Internet tra il 1984 ed il 2016*, 13 dicembre 2018, Il Sole 24 Ore.

SMART 2020: *enabling the low-carbon economy in the information age*, 2020, GeSI.

*Streaming video, è made in Italy la tecnologia "a prova di crash"*, CORCOM, 16 febbraio 2017. Articolo pubblicato su: [corrierecomunicazioni.it](http://corrierecomunicazioni.it).

*The Akamai Network: A Platform for High-Performance Internet Applications*, technical publication, Akamai-Harvard.

*The Case for a Virtualized CDN (cCDN) for Delivering Operator OTT Video*, white paper, Akamai.

*The Forrester Tech Tide: Video Technologies For Customer And Employee Experience*, Forrester, 2019.

*The Forrester Wave™: DDoS Mitigation Solutions*, Q1 2021, Forrester.

*The Internet of Things: Consumer, Industrial & Public Services 2020-2024*, aprile 2020, Juniper Research.

*TIM, Fastweb, Vodafone, and Wind: Service Degradation in Italy*, MedUX, 25 marzo 2020. Report pubblicato su: MedUX.

*Tim tiene testa alla pandemia: ricavi a 3,8 miliardi. Gubitosi: "Ottimista su rete unica"*, CORCOM, 19 maggio 2021. Articolo pubblicato su: [corrierecomunicazioni.it](http://corrierecomunicazioni.it).

Torchiani Gianluigi, *L'Edge Computing abilita sostenibilità ed efficienza energetica*, 8 aprile 2021. Articolo pubblicato su: [NetworkDigital360](http://NetworkDigital360).

*Un primo punto sull'impatto del Covid-19 tra e-commerce e media*, Cisco, 2020.

*Verso la rete dei contenuti*, notiziario tecnico, Gruppo Tim.

<https://www.akamai.com>

<https://aws.amazon.com/>

<https://www.cdnetworks.com>

<https://cloudflare.com>

<https://www.fastly.com>

<https://limelight.com>

<https://mainstreaming.tv/en/>

<https://finance.yahoo.com>

## RIASSUNTO

Stiamo entrando in una nuova fase dello sviluppo economico e sociale, frutto di un continuo e inarrestabile processo di innovazione, che ha caratterizzato nel corso degli ultimi due decenni lo sviluppo di Internet, favorendo la diffusione della *digital economy* in tutti i settori, non più legati soltanto all'ICT.

Questa trasformazione è il risultato di un processo di evoluzione ed espansione di Internet che costituisce sempre più lo strumento abilitante attorno al quale ruota qualsiasi attività, incidendo profondamente sia sui modelli di *business*, con effetti rilevanti di *disruption* di particolari settori economici, sia sulle abitudini e stili di vita dell'intera società. In questa rivoluzione tecnologica, come in tutte le precedenti, le infrastrutture sono alla base dello sviluppo economico: le tecnologie abilitanti non potrebbero esistere senza adeguate infrastrutture sottostanti.

Dalla sua introduzione agli inizi degli anni '60, Internet ha completamente cambiato la vita di miliardi di persone. Sulle reti pubbliche e private di cui si compone è transitato un traffico di dati pari a oltre 4,7 Zettabyte. La nostra concezione di Internet come risorsa affidabile ed illimitata, tuttavia, sta venendo sempre più messa a dura prova dalla diffusione globale della pandemia *coronavirus*. Le conseguenze della crisi pandemica hanno rappresentato uno straordinario *stress-test* delle infrastrutture critiche del Paese, che mette in luce un duplice aspetto. Da un lato, la tendenza all'utilizzo di processi di elaborazione dei dati nelle vicinanze in cui vengono generati (cosiddetto *edge computing*) rende la rete strettamente dipendente dalla dislocazione e dalla densità dei *server* sul territorio. Da ciò consegue che i Paesi che presentano un'infrastruttura non in grado di assicurare lo stesso livello di servizio in tutto il territorio e che hanno un numero limitato di *server* dislocati nel paese, scontino un *gap* tecnologico ed economico circa il buon funzionamento di Internet e rischiano di cedere il passo nella competizione globale. Dall'altro lato, si è reso ancor più evidente come il nostro Paese sia caratterizzato da situazioni infrastrutturali differenziate che fanno emergere diseguaglianze territoriali e impongono riflessioni di politica industriale. In Italia, infatti, è presente una forte discrepanza tra copertura infrastrutturale del territorio e penetrazione dei servizi: a fronte di livelli di copertura territoriale che potenzialmente consentono all'88,9% delle famiglie italiane di accedere a servizi Internet con velocità maggiori o uguali a 30 Mbps, solo il 37,2% di esse possiede effettivamente una simile connessione. Data questa condizione, risulta difficile per gli operatori offrire servizi qualitativamente migliori.

Il *lockdown* scaturito a seguito della pandemia da Covid-19 ha reso evidente il ruolo nevralgico svolto dalle reti di comunicazione: Internet è diventato il centro delle attività sociali, ricreative e lavorative. Nella fase di quarantena le reti hanno permesso a milioni di persone di lavorare, studiare, fare acquisti e mantenere i propri contatti sociali nonostante le restrizioni negli spostamenti. La permanenza forzata delle persone nelle proprie abitazioni ha avuto effetti notevoli sul sistema nazionale di telecomunicazioni. Nonostante sia stato osservato un deterioramento generale delle *performance* delle reti, la continuità del servizio è stata comunque ampiamente garantita, anche grazie al contributo di alcune piattaforme, come Netflix e YouTube, che hanno

alleggerito la pressione sulla rete attraverso una riduzione nella qualità dello *streaming* video, ovverosia la riduzione del *bitrate streaming*.

I dati emersi dalle varie analisi evidenziano un buono stato di salute delle infrastrutture mobili italiane, ma è necessario non rallentare lo sforzo in termini di investimenti, soprattutto in ottica 5G. Entro il 2022, infatti, si prevede che il 60% della popolazione mondiale userà Internet; saranno quindi *online* più di 35 miliardi tra *device* e connessioni. L'accesso a Internet tramite un'infrastruttura di telecomunicazioni ad alta capacità, affidabile e capillarmente diffusa rappresenta, dunque, un prerequisito essenziale per essere competitivi, a livello di sistema, nello scenario economico globale.

Solo un'infrastruttura in fibra ottica di tipo *Fiber to the Home* (FTTH), affidabile e diffusa in modo capillare, può infatti sostenere adeguatamente e con successo tali sfide. Inoltre, la qualità dell'accesso alla rete mobile, in previsione dell'avvento del 5G, difficilmente sarà separata da quello alla rete fissa, conferendo all'infrastruttura in fibra ottica un'importanza fondamentale in termini di "sistema nervoso" delle telecomunicazioni del presente e, soprattutto, del futuro. La fibra ottica fino a casa è l'unica soluzione che permetterà di avere tutta la banda necessaria anche in un futuro non immediato. Si può dire che sia un'infrastruttura definitiva: una volta posata, per aumentarne le prestazioni, basterà soltanto cambiare gli apparati agli estremi.

### **L'effetto video e la *Quality of Experience* (QoE)**

Un'altra componente essenziale che ha condizionato l'aumento esponenziale del traffico Internet è il cosiddetto effetto video. Il traffico video in tutte le forme è, infatti, aumentato drasticamente. Il video funge da motore del cambiamento favorendo la diffusione di reti e servizi sempre più performanti, in grado di soddisfare le crescenti aspettative dei consumatori. Come già osservato all'inizio del decennio 2010 negli Usa e, più di recente in Europa (2015), si sta assistendo all'esplosione dei servizi video con una crescita consistente in particolare del VoD. Il video *on Demand* (VOD), il *live streaming* (*linear tv*) e il *gaming* assieme rappresentano circa l'80% del traffico su rete IP.

Nel segmento VOD, la spinta alla banda deriva dall'aumento dei video HD (*high definition*) e UHD (*ultra-high definition*, 4K) a scapito della *standard definition* (SD). La tecnologia HD e UHD determina tale effetto perché il *bit rate* per video 4K a circa 15-18 Mbps è più del doppio del *bit rate* video HD e nove volte superiore al *bit rate* video *Standard-Definition* (SD). Il passaggio a contenuti di elevata qualità ed il progressivo abbandono dei contenuti con SD sta determinando un aumento considerevole del *Throughput* (TH), ossia la capacità di trasmissione effettiva o quantità di dati trasmessi in un'unità di tempo per cliente attivo (Mbps/cliente attivo). Per assicurare la *Quality of Experience* attesa dai consumatori e dall'IoT, sono necessari elevati valori di *throughput* e un *download time* minimo. Gli *Over The Top* (OTT), come Amazon, Facebook, Google, Netflix, per lo sviluppo del proprio *business* hanno bisogno che gli *end-user* possano fruire con adeguata QoE i contenuti e le applicazioni che essi offrono.

Avere elevati *throughput* e bassi *download time* è importante non solo per servizi video *streaming*, ma anche per il *web browsing*, poiché alla QoE sono legati incrementi dei ricavi di servizi offerti a *end-user* e *advertising*. Nell'*e-commerce*, ad esempio, un secondo di ritardo nel *download time* determina una riduzione dell'11% per quanto riguarda le pagine visitate ed una riduzione del 16% nella soddisfazione del consumatore. Ritardi come questi possono costituire in determinati casi semplici inconvenienti, ma tradursi in consistenti perdite economiche per i servizi OTT e *web browsing* e generare vere e proprie catastrofi nel caso delle automobili *driverless*.

L'*application throughput* (TH) è il parametro (KPI) che ha il maggior impatto sulla QoE. Il valore di TH è sempre più basso del *bit rate* (BR), che corrisponde alla velocità in Mbps del canale di comunicazione tra una sorgente e una destinazione e, in alcuni casi, anche molto più basso.

Per garantire all'*end-user* una QoE elevata è necessario aumentare il TH attraverso una riduzione dei valori:

- RTT: nelle reti IP è il tempo (misurato in ms) impiegato da un pacchetto per percorrere il cammino sorgente-destinazione-sorgente.
- *Packet loss*: indica il numero di pacchetti persi nel cammino sorgente-destinazione-sorgente a causa degli errori di trasmissione e delle code nei *router*. La sua riduzione è molto difficile.

A tal fine è necessario avvicinare i contenuti e le applicazioni ai clienti.

Grazie alle piattaforme di *Content Delivery* (CD), distribuite in modo capillare nella rete (*deep into the network*), si riesce ad ottenere un valore più basso di RTT e di *packet loss*. Riducendo la distanza fra il contenuto e l'*End-user* si migliora la QoE e, in molti casi, si riducono i costi.

Inoltre, attraverso l'utilizzo di piattaforme di *transparent caching*, si riduce la banda di picco sulla rete del Telco e questo diminuisce i costi della rete. Portando il contenuto o le applicazioni vicino agli *end-user* si riduce la latenza, determinando un miglioramento nelle *performance* in termini di TH, RTT, *Download Time*.

Di fronte alla necessità di migliorare la QoE, vi sono due principali approcci:

1. Approccio tradizionale dei Telco: obiettivo principale è quello di incrementare il *bit rate* e le funzionalità dei QoS. Si riscontra però in tale approccio un miglioramento della *performance* ridotto e un elevato TCO e TTM. Infatti, il miglioramento del TH è basso, il rapporto TH/*BitRate* diminuisce e il rapporto Costo/*BitRate* aumenta.
2. Approccio *Edge Computing*: attraverso la distribuzione di IP *Edge functionalities* e *Content Delivery platform* si registra un miglioramento delle *performance* con un TCO ed un TTM contenuti. In questo caso il rapporto TH/*BitRate* aumenta mentre il rapporto tra costo/*BitRate* diminuisce.

## **Approccio *edge computing***

L'*edge computing* è un'architettura IT distribuita con potenza di elaborazione decentralizzata, predisposta per le tecnologie di *mobile computing* e *Internet of Things* (IoT). Nell'*edge computing* i dati sono elaborati dal dispositivo stesso o da un computer o da un *server* locale e non sono trasmessi al *data center*. L'*edge computing* permette di accelerare i flussi di dati che vengono elaborati in tempo reale con latenza molto bassa o tendenzialmente nulla e consente alle applicazioni e ai dispositivi intelligenti di rispondere quasi istantaneamente, durante la fase di creazione, eliminando i ritardi: questi elementi risultano fondamentali per tecnologie quali le automobili a guida autonoma. L'*edge computing* consente l'elaborazione efficiente dei dati in grandi volumi in prossimità dell'origine. Ciò determina una riduzione nell'utilizzo della larghezza di banda Internet, l'eliminazione di parte dei costi e la garanzia di un uso efficace delle applicazioni in posizioni remote. Inoltre, la possibilità di elaborare i dati senza mai trasferirli nel *cloud* pubblico aggiunge un livello di sicurezza utile, in particolare, per i dati sensibili.

L'IP *edge computing* consente l'utilizzo di piattaforme di CD che possono determinare un importante aumento del TH e, nella maggior parte dei casi, un risparmio sui costi. Per questo l'obiettivo degli OTT e dei CDN *Provider* è di inserire le proprie piattaforme per la QoE (*server/cache/acceleratori*) a partire dai *Data center*, per poi entrare nei POP (*Point-of-Presence*), ossia i punti di interconnessione fra i vari segmenti della rete Telco, ed avvicinarsi il più possibile agli *end-users*. Questo bisogno di migliorare la QoE è una importante opportunità per i Telco che possono offrire agli OTT servizi di *delivery* con qualità differenziata. Per cogliere questa opportunità i Telco devono da un lato dotarsi di soluzioni idonee per assicurare *delivery* ad alta qualità (piattaforme per la QoE), dall'altro adottare nuovi modelli di interconnessione IP.

## **Le *Content Delivery Network* (CDN)**

In questo scenario, l'incapacità dei Telco di rispondere in modo tempestivo al passaggio da una situazione *voice centric* ad uno scenario *data centric* e l'inadeguatezza dei modelli di interconnessione tradizionali (*end-2-end* di tipo "*best effort*") hanno favorito l'affermazione di soggetti (es. Akamai, Limelight, CloudFlare) che offrono, a livello globale, servizi di *delivery* di traffico IP assicurando una qualità migliore di quella ottenibile con un trasporto *end-2-end* di tipo "*best effort*", ad esempio mediante soluzioni di *caching* e *web acceleration*. Tale contesto ha consentito la nascita e lo sviluppo di soggetti che si occupano di *delivery* di contenuti e applicazioni: le *Content Delivery Network* (CDN).

Una rete CDN è una piattaforma di *server* altamente distribuita che aiuta a minimizzare il ritardo nel caricamento dei contenuti delle pagine *web*, riducendo la distanza fisica e logica tra il *server* e l'utente, così da assicurare agli utenti in tutto il mondo di visualizzare gli stessi contenuti ad alta qualità senza rallentare i tempi di caricamento. Nella maggior parte delle CDN, ogni richiesta di contenuti comporta la mappatura dell'utente finale rispetto a un *server* CDN in posizione ottimale, che risponde restituendo la versione dei *file*

richiesti precedentemente memorizzata nella *cache*. Nel caso in cui i *file* non vengano individuati, il contenuto viene cercato sugli altri *server* della piattaforma CDN e la risposta viene inviata all'utente finale.

Quando il contenuto non è disponibile o risulta obsoleto, la CDN agisce da *proxy* inviando la richiesta al *server* di origine e successivamente memorizzando il contenuto recuperato per eventuali richieste future.

I servizi CDN sono essenziali per le aziende che si occupano della fornitura di contenuti agli utenti, in particolare per realtà che si occupano di:

- *Delivery* di contenuti di siti *web*.
- Diffusione e trasmissione internazionale di news.
- *Social media* che devono fornire contenuti multimediali agli utenti.
- Applicazioni di intrattenimento come Skygo, Netflix che forniscono contenuti *web* ad alta definizione in tempo reale o *On-Demand*.
- Piattaforme di *e-commerce* con milioni di clienti.
- *Gaming* con contenuti grafici a cui accedono simultaneamente utenti distribuiti geograficamente.

A seconda delle dimensioni, del *business* e delle esigenze di una azienda, i vantaggi di una CDN possono essere suddivisi in quattro diversi aspetti:

1. Miglioramento dei tempi di caricamento della pagina del sito *web* (minor latenza).

Spostando e archiviando i contenuti del sito *web* più vicino agli utenti, attraverso l'uso di un *server* CDN nelle vicinanze, i visitatori sperimentano tempi di caricamento delle pagine *web* più rapidi ed un'esperienza di navigazione migliore.

2. Riduzione dei costi per la larghezza di banda.

Ogni volta che un *server* di origine risponde a una richiesta, la larghezza di banda viene consumata. I costi del consumo di larghezza di banda rappresentano una spesa importante per le aziende. Attraverso il *caching* e altre ottimizzazioni, le CDN sono in grado di ridurre la quantità di dati che un *server* di origine deve fornire, riducendo così i costi di *hosting* per i proprietari di siti *web*.

3. Aumento della disponibilità e della ridondanza dei contenuti.

Grandi quantità di traffico *web* o guasti all'*hardware* possono interrompere il normale funzionamento del sito *web* e causare tempi di inattività. Grazie alla loro natura distribuita, le CDN possono gestire più traffico *web* e resistere a guasti *hardware* meglio di molti *server* di origine. Inoltre, se uno o più *server* CDN vanno *offline* per qualche motivo, altri *server* operativi possono raccogliere il traffico *web* e mantenere il servizio ininterrotto.

#### 4. Miglioramento della sicurezza del sito web.

Lo stesso processo con cui le CDN gestiscono i picchi di traffico può essere ideale per mitigare gli attacchi *Denial of Service* (DDoS). Si tratta di attacchi in cui gli attori malintenzionati saturano un'applicazione o i *server* di origine inviando una quantità enorme di richieste. Quando il *server* si arresta a causa del volume di traffico, il tempo di inattività può influire sulla disponibilità del sito *web* per i clienti. Una CDN agisce essenzialmente come una piattaforma di protezione e mitigazione degli attacchi DDoS attraverso GSLB (*Global Server Load Balancing*) e *server* perimetrali che distribuiscono il carico equamente su tutta la capacità della rete. Poiché la CDN è distribuita ai margini della rete, funge da barriera virtuale con un'elevata sicurezza contro gli attacchi ad un sito *web* e alle applicazioni.

Gran parte del traffico Internet viene gestito tramite CDN: nello specifico, entro il 2022, il 72% del traffico sarà trasportato tramite CDN e tale dato è destinato crescere. Le CDN sono e saranno essenziali per offrire un'esperienza di *streaming* video di alta qualità poiché aiutano a migliorare la qualità del *live streaming* distribuendo il contenuto ai *server* di *streaming* più vicini all'utente finale.

La televisione e gli OTT (Netflix, Dazn, Skygo) sono un'area altamente strategica per le CDN, perché il video in alta definizione soffre del problema della capacità di trasmissione: le reti si saturano facilmente e i *server* possono rispondere alle richieste da parte degli utenti anche con dieci, venti, trenta secondi di ritardo. Le conseguenze commerciali sono terribili. Ecco perché negli ultimi anni, con l'esplosione del video, il ruolo dei fornitori di servizi di CDN è diventato sempre più strategico.

#### **Il leader del mercato CDN: Akamai**

Akamai Technologies è stata costituita nel Delaware nel 1998, ha sede a Cambridge, Massachusetts, ed è l'azienda *leader* nel panorama delle CDN. La società fornisce soluzioni per la protezione, la distribuzione e l'ottimizzazione di contenuti e applicazioni aziendali su Internet. La piattaforma di Akamai, in continua crescita e sviluppo, rappresenta il valore aggiunto e il vero vantaggio competitivo rispetto ai *competitor*. Nel corso degli anni Akamai ha consolidato i rapporti di *peering* e ha raggiunto livelli di penetrazione con gli ISP difficilmente raggiungibili. Nessun *provider* ad oggi (Amazon, Google, Netflix, Facebook) ha la stessa struttura. Akamai da 23 anni sviluppa il proprio portfolio, garantendo scalabilità, *performance* e sicurezza elevata.

Nel 2020 ha fatto registrare un fatturato di circa 3,2 miliardi di dollari e nessun *player* nel mercato ha numeri di questa portata. Da un punto di vista finanziario, Akamai ha aumentato le entrate in ciascuno degli ultimi tre anni fiscali e nello stesso periodo ha fatto registrare una redditività positiva.

Il mercato in cui Akamai opera è estremamente competitivo e caratterizzato da tecnologie in rapido sviluppo, da *standard* di settore in evoluzione e da frequenti innovazioni di prodotti e servizi.

Si prevede che la concorrenza sui servizi offerti da Akamai aumenterà sia da parte di imprese *incumbent* sia da parte di nuovi entranti nel mercato. La competizione tra i vari *player* si basa principalmente su:

- Prestazioni e affidabilità delle soluzioni e dei servizi offerti.
- Ritorno sull'investimento in termini di risparmio sui costi e nuove opportunità di guadagno per i clienti.
- Ridotta complessità dell'infrastruttura.
- Raffinatezza e funzionalità delle offerte.
- Scalabilità.
- Sicurezza.
- Facilità di implementazione e fruizione del servizio.
- Servizio Clienti.
- Prezzo.

Akamai si trova in concorrenza con aziende che offrono prodotti e servizi che mirano a garantire elevate prestazioni Internet, con aziende che forniscono servizi di *hosting*, servizi di distribuzione di contenuti Internet, soluzioni di sicurezza, soluzioni tecnologiche utilizzate dai vettori per migliorare l'efficienza dei loro sistemi, servizi di distribuzione di contenuti in *streaming* e soluzioni basate sull'utilizzo di apparecchiature volte a risolvere i problemi relativi alle prestazioni di Internet, come bilanciatori del carico e *switch* del *server*.

Il tasso di crescita dei ricavi di cui Akamai ha goduto negli ultimi anni potrebbe non proseguire e addirittura comprimersi, causando un impatto negativo sulla redditività e sul prezzo delle azioni. Le entrate dipendono dalla quantità di traffico che viene fornito, dalla continua crescita della domanda per le prestazioni e le soluzioni di sicurezza offerte e dalla capacità di mantenere i prezzi che vengono applicati ai vari clienti. Nel 2020 Akamai ha fatto registrare un aumento significativo delle entrate derivanti dalle soluzioni multimediali, in gran parte dovuto al maggiore consumo di *media*, di giochi *online* e di ordini casalinghi durante la pandemia di COVID-19.

Numerosi altri fattori influiscono sulla crescita del traffico:

- Il ritmo di introduzione di iniziative di distribuzione video *over-the-top* (OTT) da parte dei clienti.
- La popolarità delle offerte di *streaming* dei clienti rispetto alle offerte da parte di aziende che non utilizzano le soluzioni offerte da Akamai.
- La variazione positiva della popolarità del *gaming online*.
- I *media* e altri clienti che utilizzano i propri *data center* e implementano approcci di consegna che limitano o eliminano la dipendenza da fornitori di terze parti come Akamai.
- Le condizioni macroeconomiche generali e le pressioni nel settore.

I livelli di traffico sulla rete hanno iniziato a stabilizzarsi nel quarto trimestre del 2020. Di conseguenza non si prevede che la crescita del traffico nel 2021 continuerà agli stessi livelli che sono stati registrati all'inizio del 2020, in assenza di altri sviluppi significativi del settore.

Negli ultimi anni le aziende che offrono soluzioni di sicurezza hanno fatto registrare una crescita significativa dei ricavi. Per mantenere o accelerare la crescita dei ricavi provenienti dalla sicurezza è necessario aumentare la posizione dominante di Akamai in tale ambito e sviluppare nuove soluzioni in un ambiente in cui le minacce alla sicurezza sono in continua evoluzione. L'azienda ha necessità di garantire che i propri servizi funzionino in modo efficace e che siano competitivi con i prodotti offerti da altri.

Akamai ha fatto registrare un calo dei ricavi negli ultimi trimestri relativo alle soluzioni per le prestazioni *web* e si prevede che questa tendenza continui a causa della crescente pressione sui prezzi in alcune aree geografiche, determinata dalla concorrenza e delle condizioni commerciali che interessano molti dei clienti di Akamai, nello specifico in riferimento a settori come i viaggi e l'ospitalità. Nel 2020 molti di questi clienti hanno dovuto affrontare interruzioni significative della propria attività a causa dell'emergenza sanitaria pubblica internazionale associata alla pandemia di COVID-19. Le ricadute economiche della pandemia sono proseguite nel 2021 e si prevede possano avere conseguenze di vasta portata in molti settori: fallimenti, riduzioni della spesa tecnologica e recessione economica. Ognuna di queste circostanze avrebbe un impatto negativo sui ricavi.

Altri fattori che potranno influire sui risultati di Akamai sono:

- Fidelizzazione dei clienti esistenti, mantenendo i servizi attuali e offrendo loro nuove soluzioni.
- Sviluppare e vendere nuove soluzioni innovative e accattivanti.
- Affrontare la potenziale mercificazione delle soluzioni basate sulla consegna, che può portare a prezzi più bassi e alla perdita di clienti a favore dei concorrenti.
- Contrastare le *policy multivendor* che potrebbero indurre i clienti a ridurre la loro dipendenza da Akamai.
- Adattarsi ai cambiamenti nei modelli di contratto con i clienti, da una struttura di ricavi *committed* (fissa/stabilita) a un approccio "*pay-as-you-go*".
- Gestire l'impatto dei cambiamenti nelle condizioni economiche generali.

Se Akamai non sarà in grado di aumentare i ricavi, la sua redditività e il prezzo delle azioni potranno risentirne, anche se uno dei principali rischi per Akamai, ovviamente, rimangono i *competitor*.

## I competitor di Akamai

### 1. Operatori Big tech

Akamai ha raggiunto un rapporto 1:100 rispetto alle cosiddette aziende-stato, come Facebook, Amazon, Apple, Google, Netflix. Si possono distinguere gli operatori *big tech* verticali come Netflix, che detiene le proprie infrastrutture e a seconda delle occasioni prende in prestito quote di rete da altri operatori, e *player* più differenziati come Amazon e Google, che sono caratterizzati da un *core business* e da una serie di adiacenze. Per quanto riguarda Amazon, i servizi informatici in *cloud* (ossia il *core business* di AWS) hanno ormai assunto un'importanza maggiore rispetto all'*e-commerce*, infatti pesano più della metà rispetto a quest'ultimo in termini di utili. Nel campo dei servizi informatici l'obiettivo principale di Amazon è quello di andare ad acquisire la professionalità degli sviluppatori dei codici e delle applicazioni, così da riuscire a trasformare i loro *software* e renderli facilmente integrabili con le piattaforme di Amazon stesso: è in tale contesto che il colosso americano compete maggiormente.

Amazon potrebbe ritenere strategico ampliare e sviluppare la propria infrastruttura di *content delivery* per garantire una QoE elevata agli utenti per il *live streaming* di Amazon Prime, dato che sta investendo ingenti somme nel mondo dei diritti sportivi (Premier League, Champions League).

Solitamente, grazie ai loro volumi, realtà come Amazon entrano nei mercati obiettivo in perdita e li prosciugano di risorse fissando dei prezzi ad una soglia molto bassa, riuscendo così a svuotare il mercato e a operare in un'ottica di lungo periodo.

Un discorso simile può essere fatto per Google, anche se i servizi aziendali informatici di Google hanno ancora un peso ridotto rispetto al *business* dei ricavi pubblicitari (*core business*). Infatti, i ricavi pubblicitari rappresentano circa il 90% dei ricavi totali (166 miliardi sui 182,5 totali), mentre i ricavi di Google Cloud nel 2020 ammontavano a 13,1 miliardi di dollari, in aumento (+47%) rispetto agli 8,9 miliardi di dollari del 2019 (e 5,8 miliardi nel 2018), ma questa parte di *business* risulta ancora in perdita operativa per 5,6 miliardi di dollari, evidenziando come sia ancora in modalità di investimento.

Per Akamai e più in generale per gli operatori che offrono servizi di CDN, i *big tech* sono dei *competitor*, ma non rappresentano in questo momento una minaccia poiché per loro la componente di *delivery* non è strategica. La *delivery* ha un'incidenza ridotta rispetto all'impatto che puntano ad avere con i loro *core service*. Attualmente, quindi, l'obiettivo principale di Amazon, è quello di colpire *player* come IBM e non Akamai, anche perché quando Amazon organizza *convention* a livello mondiale su piattaforma video prende in affitto i servizi di Akamai (Amazon prime usa Akamai, Apple usa Akamai).

La politica di Amazon è volta a garantire la massima soddisfazione del cliente: in base ai bisogni e alle necessità dei clienti AWS si muove nel mercato e fa investimenti. Questa strategia può essere percorsa data la grande forza finanziaria di Amazon che usa economie di scala e trasferisce i risparmi al cliente.

Akamai, invece, attualmente si sta concentrando sull'utilizzo di un *network* distribuito all'*edge* che rappresenta il suo principale *asset* strategico (*Akamai Intelligent Edge Platform*), grazie ad accordi e convenzioni con la gran parte degli operatori telefonici nel mondo. La strategia di Akamai è quella di far leva su tale *asset* per rispondere alle esigenze riguardanti la sicurezza (obiettivo *core* per Akamai).

Nello specifico, mettendo a confronto la CDN di Akamai con AWS CloudFront (CDN di Amazon) emerge come la piattaforma di Akamai sia la migliore per lo *streaming* video in diretta. Quattro sono i parametri più rilevanti da approfondire:

- **Scalabilità:** una delle metriche più importanti per una CDN di *streaming* video è la dimensione della rete, dato che più grande è la rete di cui si dispone più sono gli *endpoint* a cui è possibile indirizzare gli utenti. Akamai dispone di *server* in più di 130 paesi collegati a più di 1.700 reti. CloudFront, d'altra parte, ha più di 225 PoP. Poiché i *file* video sono di grandi dimensioni, avere più *server* distribuiti strategicamente è un grande vantaggio nella distribuzione di *streaming online*. La differenza tra Akamai e AWS CloudFront è significativa in questo campo.
- **Performance:** dalle analisi emerge che Akamai sembra avere un netto vantaggio su CloudFront quando si tratta di prestazioni. I test internazionali e un'analisi specifica del *throughput* CDN mostrano che Akamai è circa il 15% più veloce di CloudFront. Ciò è particolarmente importante per lo *streaming live* in quanto riduce i problemi di visualizzazione, come ad esempio i problemi di *buffering*.
- **Affidabilità:** ci sono due componenti principali da considerare quando si tratta di determinare l'affidabilità: disponibilità e sicurezza. Per quanto riguarda la disponibilità la differenza tra i due è insignificante, mentre per quanto riguarda la sicurezza è noto che AWS è in ritardo rispetto alla maggior parte dei *content provider*. Akamai, invece, è *leader* di mercato nella distribuzione sicura dei contenuti.
- **Prezzo:** i prezzi di CloudFront sono relativamente aggressivi. Hanno una struttura semplice, con pagamento in base al consumo, anche se ci sono molti costi aggiuntivi, che devono essere presi in considerazione. Akamai ha un sistema di prezzi più complesso, che si basa su contratti negoziati. Non è trasparente. Il prezzo dipende dalla larghezza di banda, dall'area geografica, dai tipi di traffico e dalla durata del contratto.

Non ci sono dubbi, quindi, che Akamai sia il *leader* di mercato nel contesto delle CDN con una quota di mercato del 35% basata sul fatturato annuo a livello globale. Essa serve la maggior parte delle aziende *Fortune* 500. AWS CloudFront offre comunque soluzioni molto potenti adatte per l'*hosting* di siti *web* professionali e la distribuzione di contenuti.

## 2. Operatori telefonici in forma privata e in forma condivisa e gli operatori di transiti

L'infrastruttura detenuta dagli operatori telefonici è un elemento di differenziazione e vantaggio competitivo. I Telco rappresentano, quindi, un potenziale *competitor*, ma sono maggiori i benefici di una collaborazione tra operatori di *Content Delivery* e Telco rispetto ad una *competition* tra le parti. Questo perché gli operatori di CDN raccordano grazie ai loro *software* i vari *edge* della rete e tale operazione risulta impossibile per gli operatori telefonici: difficilmente vi possono essere condivisioni di POP tra diversi operatori. I Telco vengono visti sia da Akamai che da AWS come dei clienti e in alcuni casi come dei *partner* con cui operare in simbiosi.

## 3. Operatori che si concentrano solo sulla delivery

Si tratta di operatori specializzati nel mercato delle CDN, ivi compresi le *startup*. In tale livello di *competition* è importante tenere conto delle date di avvio delle varie imprese. Consideriamo ad esempio Fastly e Limelight, aziende molto aggressive sull'offerta di *delivery* di contenuti, che tuttavia non hanno avuto il tempo e non hanno sostenuto gli investimenti necessari per costruire infrastrutture in grado di competere con Akamai. Per ordine di *market share*, anche se si parla di un ordine di grandezza 10 volte inferiore ad Akamai, i principali *competitor* di Akamai sono: Limelight, Fastly, Cloudflare e Mainstreaming. Dall'analisi dei fondamentali, al 31 dicembre 2020, emerge che solo Akamai riesce a generare utili, mentre tutte le altre aziende non sono ancora in una fase avanzata di maturità del *business*. Nello specifico, Limelight, Fastly e Cloudflare stanno sostenendo elevati investimenti che non sono ancora in grado di generare un ritorno positivo mentre Mainstreaming si trova ancora in fase di avvio/crescita.

## **Conclusioni**

Come sostenuto dal rapporto di Forrester, che analizza la maturità e il valore del *business* per 18 differenti tecnologie riguardanti il video, le CDN rientrano nel quadrante *Maintain*, caratterizzato da elevata maturità ed alto valore aziendale. Questa tecnologia è presente sul mercato da decenni e il nucleo di funzionalità è rimasto sostanzialmente invariato. Le CDN sono e saranno essenziali per offrire un'esperienza di *streaming* video di alta qualità. Gran parte del traffico Internet viene gestito tramite CDN e, nello specifico, entro il 2022, il 72% del traffico sarà trasportato tramite CDN, con un aumento significativo dal 56% del 2017. La quota di traffico gestita ai bordi della rete (*EDGE*) è quindi destinata ad aumentare progressivamente.

Data la rilevanza, la centralità e il valore delle CDN, si registreranno tentativi di entrata da parte di nuovi operatori e vi sarà una competizione molto forte all'interno del mercato, sia per quanto riguarda il prezzo che per la conquista di quote di mercato. Si tratta di un *business* in cui non sono presenti dinamiche concorrenziali come, ad esempio, nel contesto dei *social media*, nel quale l'arrivo di Tik Tok potrebbe corrispondere all'uscita dal mercato di Snapchat o Instagram. Gli *asset* di capitale, come ad esempio i *server* poggiati nei vari POP degli operatori telefonici a livello mondiale, sono il traguardo di vent'anni di progressione dell'architettura, caratterizzata da investimenti, sviluppo e crescita dell'infrastruttura.

Un vantaggio competitivo acquisito in termini di *asset* (rete, *server*, infrastrutture) è difficilmente *displaceable*. In tale contesto è quindi presente una rendita di posizione molto forte derivante dagli investimenti storici e incrementali. Infatti, se un *player* come Mainstreaming volesse offrire le stesse capacità di Akamai in Italia, dovrebbe sostenere un investimento molto elevato rispetto alle proprie possibilità economiche. Sono quindi presenti elevate barriere all'ingresso, sia dal punto di vista finanziario che dal punto di vista del *know-how*.

Tra i tre livelli di concorrenza e competizione precedentemente analizzati, le principali insidie per gli operatori di CDN già presenti nel mercato provengono dai *Big Tech*, come Amazon e Google. Infatti, queste realtà sono considerate delle aziende-stato date le loro dimensioni, i loro volumi e il fatturato, che ammonta a 386 miliardi per Amazon e 183 miliardi per Google. Dati questi numeri è evidente che nel momento in cui le *Big Tech* vogliono presidiare integralmente il mercato del *content delivery*, hanno le capacità di investimento per farlo, sostituendo Akamai (3,2 miliardi di fatturato), principale *player* nel mercato delle CDN, e, a maggior ragione, i *player* minori come Limelight, Fastly. La posizione di Akamai sembra quindi difficilmente attaccabile dagli operatori presenti nel livello 2 e 3 della *competition*, mentre risulta attaccabile dai *Big Tech*, qualora ritengano necessario per la loro strategia competitiva presidiare il mercato delle CDN.