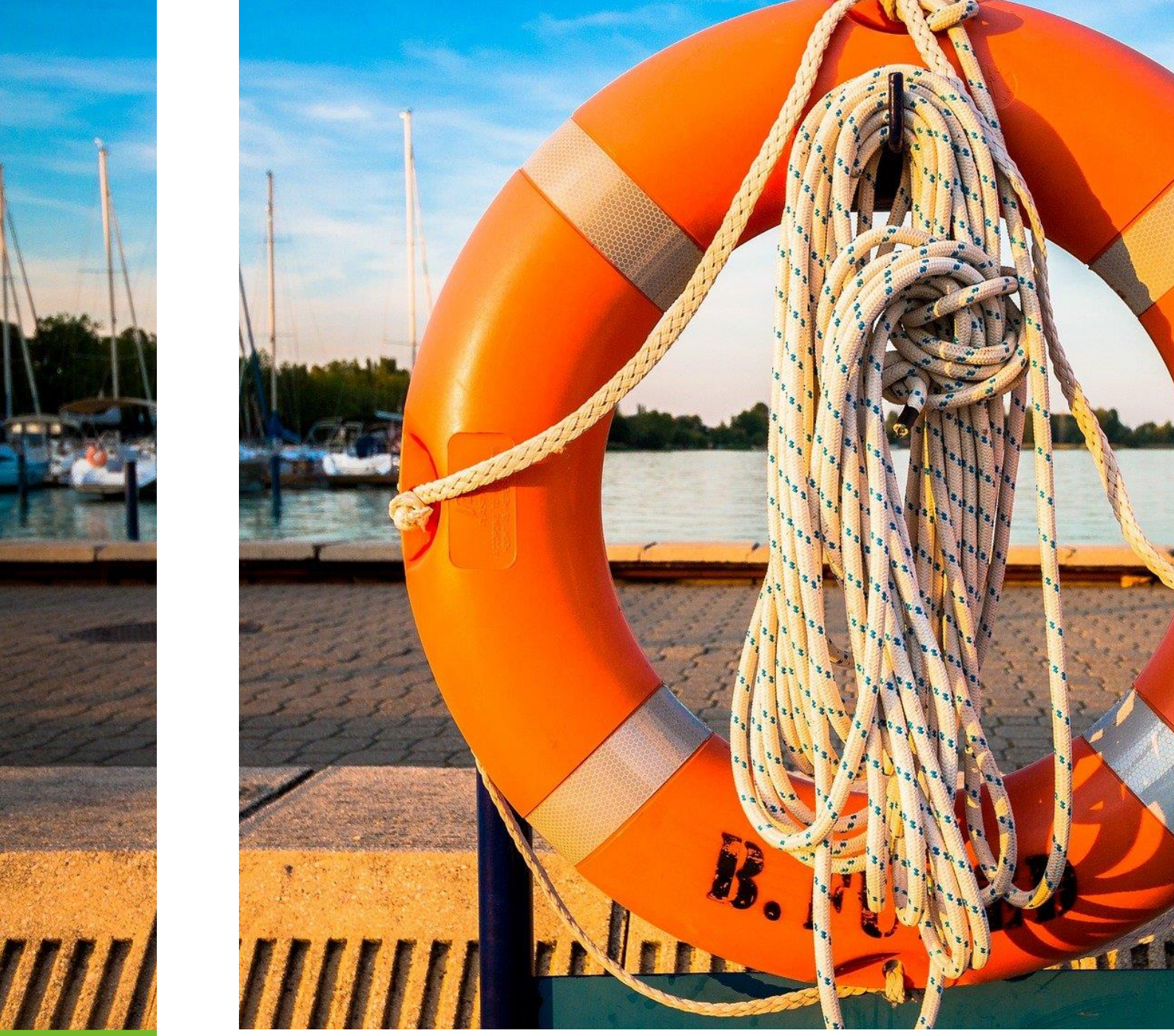


Omnisperience Discussion Paper I Teresa Cottam, Chief Analyst

Unleashing new revenue streams and boosting digital confidence with CCAPS

As the world becomes ever-more connected and a wider range of services are provided online, a seamless and robust connection is no longer sufficient. Connected customers also need the assurance their connected experience will be as expected, and that they are protected from the risks that continue to multiply as the digital environment becomes more complex.

Connected Customer Assurance & Protection Services (CCAPS) meet these requirements by eliminating the gaps between current security applications, removing customer effort, and providing unobtrusive but more effective protection for all devices, connections, personal data and activities. CCAPS support digital confidence in the Work Anywhere, Connect Everywhere era, while generating a long-term increase in CSPs' ARPUs.

Omnisperience
value from experience

"CCAPS underpin the connected experience and offer immediate and achievable new revenue that bridges the gap until other promising services mature."

Teresa Cottam, Chief Analyst, Omnisperience

CONTENTS

TERMS

ARPU	average revenue per user
CCAPS	connected customer assurance & protection services
CISO	chief information security officer
CPE	customer premises equipment (eg routers or media boxes)
CSPs	communication service providers
Gig Economy	a working model whereby workers take short-term contracts as self-employed workers, enabled by digital platfoms that bring employer and employee together
LAN	local area network (the network inside a home or office)
WAN	wide area network (eg the mobile or broadband network)
Work Anywhere	a model whereby people work partly from home, partly from a central workplace and partly from other places

The Work Anywhere, Connect Everywhere paradigm obsoletes legacy cybersecurity models

The COVID-19 crisis challenged businesses to rapidly adapt and accelerate their digitalisation. They responded well from a business continuity perspective. Workforces were rapidly relocated to work from home, new digital tools were deployed, and networks coped.

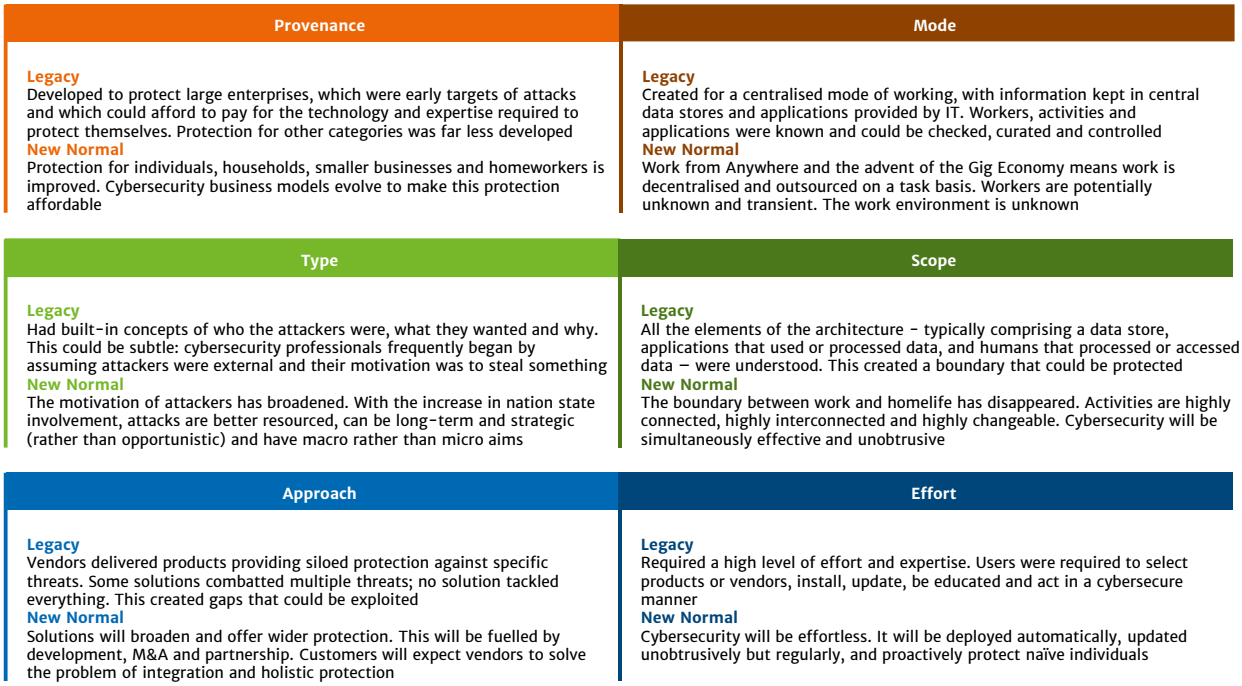
Cyber criminals did not sit on their hands, however, but quickly capitalised on the gaps left by rapid change, the fear and naïveté of ordinary workers, as well as the opportunity afforded by cybersecurity teams being depleted, stretched or redeployed to help 'keep the lights on'.

The result was a huge increase in phishing and ransomware attacks, with the FBI reporting a 300% increase in cybercrime in April 2020 alone. Worryingly, not only had there been a hasty implementation of new technologies with little opportunity to analyse any vulnerabilities created but, as the FBI noted, attackers' motives have shifted. While criminality and cyberterrorism persist, attacks are increasingly being weaponised by nation states to further their own interests. These attacks are more organised, far better resourced than those of the average cybercriminal, have a broader scope and, as the Solar Winds attack demonstrated, their motivation is more strategic than previous tactical attacks.

Johnson & Johnson's CISO, Marene Allison, noted that pharmaceutical firms were specifically targetted in 2020, experiencing attacks "every single minute of every single day", by those seeking to steal vaccine know-how.

Such threats are not only serious but have finally obsoleted many assumptions that still underpin legacy cybersecurity practices. These assumptions have led to structural problems within the industry and in our approach to cybersecurity and urgently need rethinking (see *Figure 1*).

Figure 1 Assumptions in legacy cybersecurity models challenged by the new mode of working and living



HOW CCAPS CLOSE THE CYBERSECURITY GAPS

Gaps are one of the biggest challenges the cybersecurity world currently faces, as each gap provides an opportunity for attackers to exploit. Some of these gaps are well understood; others have either emerged recently or become more significant.

8 key assurance & protection gaps

- The functional gap - between different cybersecurity products that attackers can utilise
- The domain gap between B2C and B2B cybersecurity products now that home and worklife have blurred
- The coverage gap that means certain locations, devices and networks are protected and others are not
- The knowledge gap about risks and threats
- The expertise gap resulting from there being insufficient skilled cybersecurity practitioners
- The affordability gap which makes more sophisticated technology unaffordable for small businesses and households
- The procrastination gap resulting from customers being required to make an effort to install or update products
- The performance gap which means the expected connected performance is not delivered because the network is compromised, or devices and applications are not running optimally

How CCAPS close the gaps

Connected Customer Assurance and Protection Services (CCAPS) are a type of value-added service that Omnisperience calls 'network-plus' services. Such services are closely related to the CSPs' knowledge and control of the network and are supplied alongside network connectivity to add value to the network experience.

CCAPS are delivered as an integral part of the connected experience, securing and assuring the connected lifestyle and putting the customer at its heart rather than specific devices, data stores or applications. CCAPS sit alongside enterprise security products that secure the data and activities of large complex businesses, to close the legacy cybersecurity gaps for smaller businesses, homeworkers and households. They provide holistic assurance & protection, close the gap between B2B and B2C services, and remove the requirement for customer effort, knowledge or expertise.

Why CSPs are ideally placed to deliver CCAPS

The unique knowledge and/or control of certain key elements within the connected world make CSPs ideally positioned to deliver CCAPS.

For example, they have control and/or in-depth knowledge of wide area networks (WANs) and devices. This enables them to assure quality of service (QoS); intercept attacks while malware is still transiting the WAN and before it reaches gateways, devices and local area networks (LANs); and deploy automatic protection to any device connected to their networks.

CSPs are well placed to secure customer premises equipment (CPE) and thus the smart objects and devices connected to the home network beyond the gateway. Their knowledge of devices includes the ability to remotely diagnose faults and thus, by extension, monitor for any signs of misuse and fix any problems. In addition, Edge computing processes data locally, reducing the risk of data being intercepted or misused, and supporting assurance by boosting performance.

One of the key issues that has emerged in 2020 is that the complex chain of applications used to secure businesses and public sector organisations mean it is hard to assign responsibility for security. In contrast, CSPs are in a good and trusted position to create and support a holistic assurance & protection service that comes with an added service wrap. CCAPS also reduce the number of supplier and billing relationships for small businesses and households and consolidate charges on one bill.

Benefits of CCAPS

- Increased revenues - CSPs can quickly create a lucrative new revenue stream that increases ARPU.
- Indirect revenue boost - additional services can be wrapped around the CCAPS offering and, when customers feel more confident to connect, they're more likely to use more core and additional services.
- Improved differentiation – increased safety and performance help provide tangible differentiation from rivals based on a high quality and trusted network experience. CCAPS are thus an important element of differentiating a high-quality network.
- Innovation support – by addressing safety concerns, CCAPS remove key barriers to innovation adoption – shortening time-to-revenue.
- Encourages on-net activity - customers are more likely to remain on a safe and high-quality network, increasing their consumption of on-net bandwidth and CSPs' customer visibility.
- Better customer experience and increased stickiness – CCAPS meets customers' expectations of safety and performance, reducing their inclination to churn.

Connected customer assurance & protection services

provide digital confidence by protecting customers' devices, connections, activities, applications, data, identity and privacy wherever they are

What are CCAPS?

Connected customer assurance and protection (CCAP) services are cybersecurity services delivered through the network, as-a-service, providing holistic protection for connected customers. They are a hybridisation and evolution of B2C protection and solutions traditionally aimed at small businesses.

What are their aims?

The aims of CCAPS are to provide better and affordable cybersecurity services by automatically protecting devices, connections, activities, applications, data, identity and privacy as customers navigate the connected world.

What is their scope?

The scope of CCAPs is to protect individuals, households, small and medium-sized enterprises (SMEs), micro-businesses, nanobusinesses, and home workers. They sit alongside enterprise cybersecurity solutions and plug the gap between the smart lifespace and smart workspace. They encompass the security, privacy and performance domains.

How are they delivered?

CCAPS are automatically delivered as a service through the network by the network service provider. They are a 'network-plus' service which provides a monetisable and differentiated element to a quality network experience.

How are they different to traditional cybersecurity solutions?

CCAPS differ from enterprise solutions in 4 key aspects: (1) they are effortless and fully automated (2) they are affordable for small businesses, individuals and households (3) they are delivered by the network provider not a third-party vendor (4) they combine the traditionally separate domains of cybersecurity, network assurance and privacy protection.

CSP BUSINESS MODEL FOR PROVIDING CCAPS

CCAPS represent a significant opportunity for CSPs. Unlike some of the new potential sources of revenue for the telecoms industry, these services can be delivered today, are appealing to customers and result in an immediate boost to ARPU. CCAPS are delivered automatically with network connectivity, making CSPs ideally placed to provide them. But how does the business model for CCAPS work?

Substitute spending

CCAPS substitute for existing standalone spend on B2C cybersecurity products, but add extra value that B2C cybersecurity vendors have struggled to add or articulate. The current price for B2C cybersecurity products indicates the potential uplift for CSP offerings (see *Figure 2*).

Although marketed as solutions incorporating more than one type of protection, such offers tend to be sold on the number of devices protected. This complicates the sale for customers, as they have to estimate how many licences to buy, and builds gaps into the service model, as there may very well be additional devices within the household not covered by the offering. B2C products usually feature an 'offer' period, after which the service renews at a higher price and usually requires a yearly licence to be purchased upfront. In addition, exactly what's included within the solution varies, with add-ons (such as VPNs) being charged in addition to the base price.

Figure 2 Pricing for B2C cybersecurity

Vendor	Low	Mid	High
Avast Premium	£34.99 1 device	N/A	£39.99 10 devices
Kaspersky Total Security	£19.99 1 device	£29.99 5 devices	£39.99 10 devices
MacAfee Total Protection	£29.99 1 device	£34.99 5 devices	£39.99 10 devices
Norton 360	£24.99 1 device	£24.99 5 devices	£44.99 10 devices
TotalAV Total Security	N/A	N/A	£59.00 6 devices

Prices correct in January 2021

Business model for CCAPS

CCAPS unlock and underpin significant additional revenue for CSPs, as well as meeting customer expectations, providing confidence in the connected world and helping differentiate network services. In terms of direct revenue, however, how much revenue should CSPs expect them to generate? As indicated, the substitution spend indicates that they should be able to generate $1-3/£1-3/€1-3 per month in recurring revenue. This is confirmed by the experience of CSPs that have already rolled out basic CCAPS.

Research by Coleman Parkes found that consumers might be willing to pay even more. Its research found 74% of APAC consumers were willing to pay $4.81 per month for such services; LATAM consumers $5.50; and US consumers $4.80. ('CSP Security Survey: Trends in the US, Japan and LATAM', September 2020)

But what proportion of customers can be expected to buy such services? Again, experience suggests it's an attractive offer as it simplifies consumers' buying experience and isn't costing them much extra money. When well-marketed, CSPs can expect to see up to 50% take up in their customer base.

As *Figure 3* shows, CSPs could realise significant and highly profitable new revenue streams from CCAPS. While the cost of delivering these services is minimal, because they're delivered to existing customers out-of-the-network, it should be remembered that where a CSP is using third-party software there will be an associated cost or revenue-sharing agreement to account for. However, even if this is the case, potential returns are still substantial when this model is applied to the customer base of a large tier 0 or tier 1 CSP.

Evolving the business model

Not all current solutions include all aspects of CCAPS across the five centres of excellence outlined, providing scope to widen the offering and increase the value delivered. CCAPS can also be broadened into a differentiated QoS offer, insurance can be added, or a fully managed service can be provided for smart households (including fault detection and repair, smart-object-as-a-service and so on).

Figure 3 CCAPS boost to ARPU, per year per 10m customers

Uptake scenario	Increase in ARPU €1	Increase in ARPU €2	Increase in ARPU €3
Low 10%	12 million	24 million	36 million
Mid 25%	30 million	60 million	90 million
High 50%	60 million	120 million	180 million

"CCAPS are not just a killer service, they're a serial killer service."

Teresa Cottam, Chief Analyst, Omnisperience

Five Fresh Ideas
You Should Now Know

1

CCAPS offer the possibility of virtually instant revenue with high margins. They also underpin emerging revenue streams.

2

CSPs are uniquely placed to offer a holistic assurance, performance and cybersecurity service, taking household and SME revenue share from third-party vendors.

3

CCAPS simplify the security proposition for small businesses and households by combining assurance and protection with network provision and enabling them to pay monthly via a single bill.

4

CSPs do not need to self-develop these solutions but can assemble the necessary components from third-party vendors. They can reduce risk through revenue-sharing arrangements with vendors.

5

CCAPS can be launched as a fairly straightforward assurance and protection service and expanded to include more features over time. Additional elements to the service include insurance against damage and downtime; fully managed smart home services that detect and fix faults and provide smart objects as-a-service; media verification & protection.

The author

Teresa Cottam |
Chief Analyst |
tc@omnisperience.com

Teresa leads our research & analysis. She is a renowned expert on connected experience and telecoms business models. She is a judge of the GSMA's Global Mobile Awards (GloMo's), the World Communication Awards and for the UK Cloud Awards.

She previously held senior positions at Telesperience, Analysys Mason, Chorleywood Consulting, Informa and Ovum.

Omnisperience

Omnisperience is a new analyst firm that takes a fresh approach to research and advisory projects, helping our customers better understand their market and, as a result, become more profitable.

Our experienced analysts focus on digital service providers in the telecoms, media & technology sector (TMT), providing insight that helps them reimagine their businesses and improve their commercial success.

Omnisperience engages and inspires, delivering **Value From Experience.**

This paper

Omnisperience **Green Papers** are intended to define new concepts, provoke fresh thinking and stimulate further discussion. They are often the precursor to more in-depth work.

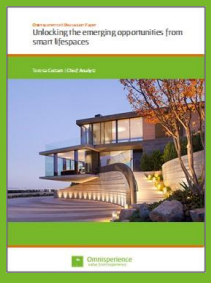
You may circulate this paper to your peers and customers. You may also re-use content from it, provided you attribute it to Omnisperience.

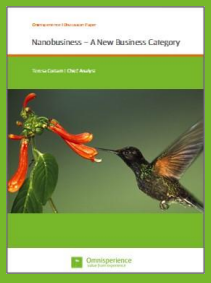
Feedback and editorial enquiries about this paper should be sent to Teresa Cottam. Those wishing to sponsor additional thought leadership on this topic should contact Sami Gharres sg@omnisperience.com

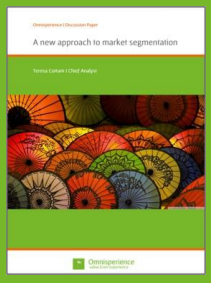
Website: omnisperience.com
Email: editorial@omnisperience.com

Check out our website for more complimentary papers.

Omnisperience, 71–75 Shelton Street,
Covent Garden, London WC2H 9JQ







Omnisperience
value from experience