THE GLOBAL MARKET OPPORTUNITY FOR CARRIERS IN PROTECTING THE DIGITAL FAMILY

avast

JUNIPER RESEARCH

Executive Summary

Value-added security solutions provide the opportunity for carriers to deliver an array of services to families worldwide. They can provide consumers with:

- Insights into their family's online behaviour, allowing parents to become better informed and sufficiently empowered to set limits appropriately.
- Greater peace of mind, via features that do not simply impose controls, but enable visibility on the places their family goes on and offline.
- Protection from online threats in the form of malware, fake apps, and data leakage.

At the same time, parents will increasingly look to carriers to provide a safe environment in which their children can work, play and communicate online. By deploying these solutions, carriers can demonstrate both leadership and social responsibility, while at the same time generating additional revenue streams. These solutions can be a strong driver of sticky family plans, and provide a gateway to more bundled services like smart home protection, extending controls, insights and digital security to all connected devices.

1. Introduction – Safety in the Connected Family

With consumer devices in the home increasingly connected and a sharp rise in child ownership of, and access to, connected devices, there is now a greater risk both of devices being hacked and/or exposed to malware, and of children accessing inappropriate content.

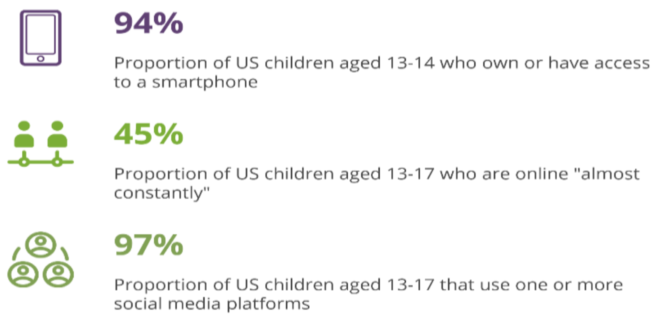
Parents are also concerned at how much time their children are spending online, and what impact high levels of screen time might have on their development. These 21st century worries only serve to exacerbate more traditional concerns, such as where their children are at a given time.

This White Paper explains these concerns in more depth and demonstrates how mobile applications can help to alleviate them, by providing parents with control over the content their children access, insights on that content and knowledge of their children's whereabouts, together with protection from malware.

1.1 What Children May be Watching… and Who May be Watching Them

Children using the Internet may be exposed to a host of inappropriate content, online gambling and unwanted influencers.

Figure 1: US Children, Key Device Ownership & Engagement Metrics, 2018



94%

Proportion of US children aged 13-14 who own or have access to a smartphone

45%

Proportion of US children aged 13-17 who are online "almost constantly"

97%

Proportion of US children aged 13-17 that use one or more social media platforms

Source: Juniper Research based on data from Pew Research Center (May 2018)

In some instances, children risk coming into contact with cyberbullies and adult content.

A host of studies have demonstrated the extent of the problem. A 2016 study by Middlesex University commissioned by the NSPCC found that 53% of UK children aged 11-16 had viewed pornographic material online.[1] In the same year, a report from the Cyberbullying Research Center in the US found that just under 34% of teens reported they were victims of cyberbullying.[2]

Furthermore, the challenges are being exacerbated by the sheer variety of ways by which children can access online content and services, both inside and outside the home. In addition to smartphones, many young children and teens now possess their own tablets and/or laptop devices; the number of online touchpoints is growing steadily and inexorably.

Understandably, parents are concerned about how to counteract these threats. A survey of parents with children aged 5-15 published in 2017 by the UK media regulator Ofcom, found that 40% were worried that their children would be exposed to cyberbullying online; 39% were concerned that their child might give out personal details to inappropriate people (39%); 35% worried that their children might view inappropriate content. In all cases these percentages had risen since the equivalent survey 12 months' previously.[3]

Figure 2: UK Children, Key Device Ownership & Engagement Metrics, 2017

83%

Proportion of UK children aged 12-15 who own smartphones

55%

Proportion of UK children aged 12-15 who own tablets

74%

Proportion of UK children aged 12-15 who have a social media profile

21 hours

Average time spent online per week by UK children aged 12-15

Source: Juniper Research based on data from Ofcom study (November 2017)

1.2 The Impact of Excessive Screen Time

At the same time, there is increased concern about the implications of too much screen time, ranging from its impact on a child's mental health to a child's ability to perform well at school.

Research published in the journal *Clinical Psychological Science* in November 2017 (with a sample size of more than 500,000) found that adolescents who spent more time on new media (including social media and electronic devices such as smartphones) were more likely to report

[1] https://www.bbc.co.uk/news/education-36527681

[2] https://www.comparitech.com/internet-providers/cyberbullying-statistics/

[3] https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

mental health issues, with those who spent more than 5 hours per day on electronic devices having almost twice the suicidal tendencies of those spent an hour or less per day.

More recently, an academic study of 4,520 US children, published in *The Lancet* in September 2018, found an association between the amount of screen time and child cognition levels, with children aged 8-11 who spent less than 2 hours per day on recreational screen time performing better in tests of mental ability.[4]

Given both the scale of the problems and the extent of parental concern, there is a clear opportunity for connected service providers to address them through the provision of family security services.

As this White Paper will make clear, these products can demonstrably offer tangible benefits for both children and parent consumers alike.

2. Benefits for Consumers

2.1 The Comfort of Control

Amongst consumers, there has been a greater willingness to embrace and adopt platforms enabling visibility on, and control of, the connected family, thereby allowing customers to protect their home and families. Control-based platforms not only allow adults to assign permissions on data usage and content (and thereby to schedule data downtimes during school hours and bedtime), but to gain greater visibility on what minors (and even seniors) are doing online.

Certainly, there appears to be a growing awareness amongst parents that it is their responsibility to control their children’s access to connected devices and content. A survey, conducted in late January 2018 by Common Sense Media and SurveyMonkey, of more than 4,200 US adults (including more than 1,000 parents of children under 18) found that 89% of parents believe that it is up to them to curb their children's smartphone usage.[5]

Furthermore, significant numbers of parents believe that the implementation of controls that restrict screentime and block access to inappropriate content are key to curbing overuse and over exposure. A Nielsen survey run in Q4 2016 (sample size: 4,636 parents of children aged 6-12) found that 55% felt their concerns could be addressed by better safety controls and features to block inappropriate content, while 48% felt similarly about better usage controls to limit access.[6]

Meanwhile, greater peace of mind can be afforded by features that do not simply impose controls, but provide insights into the children’s mobile device usage.

2.2 Understand What Children are Watching…

Many parents admit that their knowledge of what their children are doing when online is partial at best.

[4] https://www.thelancet.com/journals/lanchi/article/PIIS2352-4642(18)30278-5/fulltext
[5] https://eu.usatoday.com/story/tech/talkingtech/2018/02/22/exclusive-nearly-half-parents-worry-child -addicted-mobile-devices/362184002/
[6] https://www.nielsen.com/us/en/insights/news/2017/mobile-kids--the-parent-the-child-and-the-smartphone.html

An October 2017 survey by Common Sense Media and Survey Monkey found that 48% of US parents had only limited awareness of what their teenage children were watching or doing online.[7]

In many cases, children are likely to be playing games which are age inappropriate. For example, *Fortnite* (PEGI-rated 12 in the UK) is an online shooter game in which 100 players fight it out to be the last person standing. In September 2018, it had nearly 80 million players, many of whom are believed to be below the game's recommended age requirement. Worryingly, a 2017 survey of more than 2,000 UK parents by childcare also found that nearly half (43%) of parents had seen a negative change in their child's behaviour since playing games aimed at adults.[8]

Solutions that go beyond control to enable parental visibility on the nature of the content their children are consuming are therefore likely to be particularly attractive. Such solutions can offer parents both a greater awareness and a greater understanding of how their children engage with content.

This in turn may give parents a greater understanding (and awareness) of the kind of content that their children are consuming. Parents who are better informed about what the children are doing, and when they are doing it, can feel sufficiently empowered to make decisions about whether content being viewed is suitable and, if so, whether the time being spent engaging with it is excessive.

2.3 … And Gain Greater Insight into Usage Patterns

Best-in-class apps go beyond visibility to provide extensive insights into the content and applications being accessed, into the permissions which specific apps have on a connected device, and into usage patterns. However, perhaps more importantly, they provide insight into how any given family's usage compares to others' of similar demographics or geography.

These insights enable a radically different dynamic in the conversations between parent and child, allowing the former to have informed discussions with their children about how they are using their connected devices, and whether the content and level of content consumption is appropriate.

They are then in a far better position to agree on an appropriate length of time that their children can use their device. and what they should be using it for. Indeed, these insights can also be used as a means of enabling the whole family to think about the best way to use the Internet.

2.4 Protect Against Malware

While parents' chief concerns centre on content and control, fears of malware are never far behind.

The surge in consumer connected devices has, in turn, led to a dramatic rise in the scale of cyberattacks directed at the consumer market. Malware, spoofing, ransomware and phishing attacks have soared, with fraudsters keen to exploit any weaknesses to acquire personal

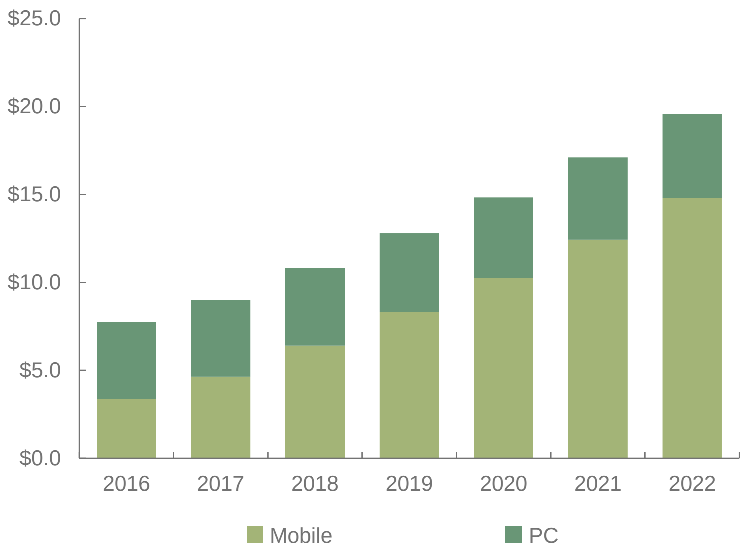
[7] https://www.commonsensemedia.org/sites/default/files/uploads/research/commonsense-surveymonkey_teeninternetuse-topline_release.pdf
[8] https://www.childcare.co.uk/blog/video-games

information such as bank account details or, in some cases, to engage in full-blown digital identity theft.

One of the most common threats in this regard is ‘downloaders', which allow apps to install additional, unwanted apps (and, potentially, malware) on smartphones. This malware can then be used to steal a user's passwords and credit card data.

For example, Juniper Research estimates that the value of online payment fraud in eRetail in 2018 as a result of these attacks was $10.8 billion, of which nearly 60% occurred via mobile devices.

Figure 3: Value of Annual Global eRetail Fraud ($bn), 2016-2022



Source: Juniper Research

Furthermore, mobile phones infected with malware can provide hackers with a compromised entry-point to the rest of a home’s network when connected to Wi-Fi. Hence, any platform that can safeguard consumer devices not only from content but also digital threats will be an attractive proposition for consumers. Later, we will discuss how security providers are extending mobile controls and security to the home network.

2.5 Know Where Their Children Are

Although the concerns outlined above stem exclusively from the emergence of connected devices, it should be observed that these devices also offer solutions to more traditional worries. Parents are able to check their family’s location, set-up time-based geofences and common safe areas.

Understandably, parents don’t want to be glued to their phones, marking their child’s every movement. Here the benefits of a safety application with AI (Artificial Intelligence)-driven anomaly alerts comes into play.

For example, if a child was supposed to be in school at a given time and her device indicates that she is at a different location, the safety application would recognise this as an anomalous location and an alert would be sent to the parent to inform them of this fact, without the parent having to set up a geofence.

Having visibility on the physical location contributes to the trust and peace of mind that children (or elderly parents) are safe.

3. Benefits for Carriers

Why should carriers care? We would argue that carriers can derive numerous benefits from digital safety solutions, namely:

- A new revenue stream;
- A reduction in churn and retention costs;
- The opportunity to acquire more customers on higher value family plans;
- Increased levels of trust with their customers;
- An opportunity to fulfil their social obligations;
- An opportunity to capitalise on their seamless billing capabilities to deliver an attractive service with minimal friction.

The following sections outline these benefits in greater detail.

3.1 Operators Need New Revenue Streams; Safety Can Deliver One

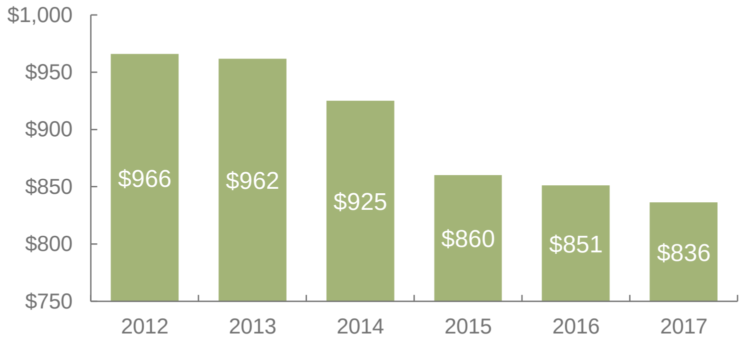
Most operators have seen revenues from traditional, core services such as voice and messaging decline. Markets are effectively saturated, meaning that there are limited new customers for operators to chase. At the same time, those markets have become increasingly competitive, with multiple MVNOs (Mobile Virtual Network Operators) fighting for market share with the network operators and driving down prices.

An additional factor here is that social media substitution has also had a detrimental effect on revenue levels, with consumers often preferring to communicate via Facebook or Instagram rather than calls. At the same time, OTT messaging platforms have soared in popularity; in 2017, 55 billion messages were sent on WhatsApp alone, compared with less than 16 billion text messages.

Furthermore, some operators have also seen revenues squeezed by regulatory intervention. For example, the European Commission has imposed a series of restrictions on MNOs regarding the rates consumers could be charged for voice, text and data usage while roaming on networks in other EU countries. In mid 2017, intra-EU surcharges were abolished and MNOs were only able to charge national rates.

As a result of this, roaming revenues generated by MNOs in West Europe declined from $23.3 billion in 2015 to just over $12.2 billion in 2017 as the abolition of the surcharge took effect. In 2017, operator-billed revenues had fallen to 87% of their 2012 peak levels; in West Europe, revenues are now just 58% of their 2008 ceiling.

Figure 4: Annual Global MNO Revenues ($bn), 2012-2017



Source: Juniper Research

The second part of the problem lies in the fact that, at the same time that core revenues are falling, costs, both capex and opex, are rising. To meet the demands of consumers and enterprises, MNOs must upgrade their networks to offer 4G and 5G services, thereby paying for both new spectrum and new infrastructure. During this transition (and beyond) they must cope with the surge of traffic engendered by the consumer smartphone boom, which has implications both from a network congestion and cost perspective. Furthermore, as MNOs find themselves obliged to expand both the breadth and depth of their network coverage, they can find themselves incurring far greater operating costs, ranging from site leasing expenses to electricity costs.

The net result of a combination of rising costs and falling revenues is that margins have shrunk significantly. It is therefore imperative for operators to develop new revenue streams to redress the balance. Value-added services, such as family safety, can provide carriers with customer-oriented revenue drivers to offset increased market saturation and competition.

3.2 Reduce Retention Costs

In saturated markets, there is relatively little scope for new acquisitions and hence operators are obliged to allocate significant resources to retention.

Customer retention carries a considerable cost. In 2016, two Canadian mobile operators, Bell Canada and Telus, indicated that it was equivalent to 13.2% and 14.7% of customer revenues.

By marketing bolt-ons, carriers can offer a compelling service above and beyond voice and data. These can reduce churn, by providing a differentiator from competing offerings.

This in turn allows carriers either to reduce spend on retention or translate that spend into a greater return on investment, thereby improving margins.

This could be a clear benefit in markets which are at, or near, saturation. For example, in the US, postpaid monthly churn rates for the leading carriers are currently at, or around, 1.0-1.5%, percentages that are replicated in many markets across Europe and East Asia.

3.3 Family Accounts are High Value

As markets have become increasingly competitive, carriers have sought to migrate from single user to shared accounts, thereby increasing value and reducing the likelihood of churn (as it would require all individuals in the family to migrate to a new carrier).

As of December 2017, around 90% of AT&T postpaid subscriptions were on shared accounts. AT&T stated at the time that nearly 40% of shared accounts used 15GB or more per account, implying that each of these ‘higher-end’ accounts was generating a minimum of $130 per month. This compares with AT&T’s monthly ARPU of just $47.

Furthermore, we believe that while only the US has thus far embraced the family plan approach, it is a model which is likely to gain greater traction elsewhere given its high value and relative stickiness. Indeed, we would argue that carriers which offer family safety solutions as an option with a family plan, would actually make such plans more attractive to consumers, supporting customer acquisition.

3.4 Carriers Have a Trusted Relationship with Consumers

Carriers should also recognise that the depth of their relationship with consumers places them in pole position to offer and capitalise on the deployment of digital safety solutions. In July 2018, Openet published the results of a survey of 1,500 consumers across the UK, the US, Brazil and the Philippines on their perceptions of digital services companies and mobile operators following the recent data scandal. The survey found that 56% of consumers now see their operator as more trustworthy than a digital services company.[9] Meanwhile, 92% of those surveyed said that they would be open to their mobile operator delivering digital services.

Indeed, there is a strong case for arguing that the addition of digital safety solutions would serve to reinforce the trust relationship between consumer and carrier.

Critically, carriers also have numerous technological advantages over their rivals when it comes to deployment. Perhaps the most important here is their capability to offer cross-platform solutions, a capability lacking in OS providers.

3.5 Carriers Have a Social Conscience

As the scale of consumer (and media) concerns about the nature of children's engagement with online content increases, carriers are becoming aware that they, as well as the content producers and providers, have moral obligations to deliver a safer environment for that engagement. This has been described as the emergence of a 'social conscience'.

By offering family safety solutions carriers can demonstrate the depth of their commitment to protecting their customers and helping consumers be better stewards of their families' online lives.

Furthermore, the Internet is not static: it is constantly evolving, and carriers need to evolve with it, to understand the changing nature of the risks it brings.

Parents will increasingly look to carriers to provide a safe environment in which their children can work, play and communicate online. By providing digital safety platforms, carriers can fulfil these obligations and thereby enable parents in turn to develop more awareness (and more appropriate responses) to their child's online activity.

3.6 Seamless Billing and Management

Finally, the key assets of the network operator are its network and its billing relationship with the end user. Tier 1 carriers often have tens of millions of such billing relationships. While historically the only services billed were traditional voice and data, operators have increasingly offered consumers an array of additional options which can be paid for via the bill, ranging from tickets to digital goods.

[9] https://www.realwire.com/releases/Faltering-consumer-trust-creates-window-of-opportunity-for-Mobile-Operators

In the case of digital safety services, the option is similarly billed to the phone bill and displayed as an item viewable both online and (if still requested) on the paper phone bill.

Meanwhile, in addition to online payment viewing, permissions/settings can be managed simply online by designated customers, reducing friction for both carriers and consumers.

4. The Carrier Opportunity

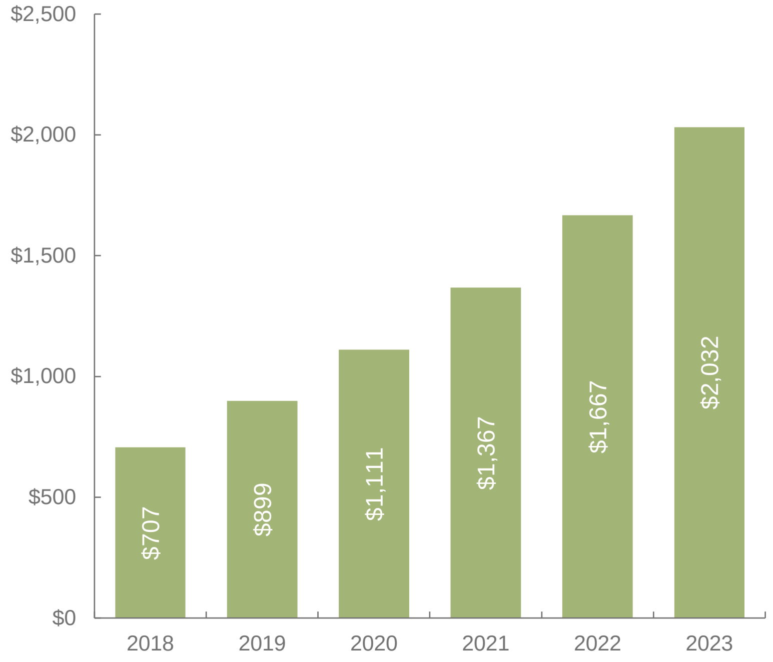
We firmly believe that there is a significant opportunity for carriers to generate substantial additional revenues from the implementation of digital safety solutions. This can either be in the form of 'bolt-ons' to existing subscriptions, or bundling with packages as a differentiator to competitors.

Juniper Research estimates that, in 2018, carriers generated approximately $700 million from such packages, primarily in the US (where family plans are well marketed and popular with consumers), Japan and South Korea.

However, we would argue that a number of key drivers should mean that global revenue streams increase to more than $2.0 billion by 2023.

- Greater child ownership of connected devices: In 2018, Juniper estimates that one or more children owned one or more connected devices in 27% of households worldwide, a figure that rises to more than 40% in many European and Asian markets and more than 60% in the US. By 2023, the global figure will be 40%. This means that, worldwide the number of households with 'connected children' will increase from just under 300 million to 450 million, thereby increasing the potential addressable base for such solutions by more than 50%.
- Greater extent of child online engagement: Most everyday activities, shopping, communication, infotainment, have steadily migrated to an online environment, for children as well as adults. While these trends are expected to continue, parents are increasingly aware that these activities pose risks to the children and will in turn look to carriers to mitigate them.
- Parental need of greater understanding of, and insight on, their children's online activities: As we have observed earlier in this White Paper, most parents lack a fundamental understanding of what children are doing and watching on their connected devices. We would argue that as more platforms are made available by carriers which enable greater insights into child online activities, then parents will be keen to utilise them.

Figure 5: Annual Carrier Revenues ($m) from Digital Safety Solutions, 2018-2023



Source: Juniper Research

- In most cases, we have envisaged that consumer monthly spend on these platforms will be around $2.50-$5.00 in developed markets, but less than $1 in markets with lower GDP and consequently lower monthly ARPU levels.
- Prices are also typically higher where the service is offered as a bolt-on to a family plan.
- We have also assumed a marginal increase in monthly subscription costs over time, as increased market competition is offset by a greater range of safety features in new service iterations.
- In some markets (such as Japan and Korea), where services are either mandated or a basic service is freely available, we have assumed that some consumers will migrate to a premium service in the latter half of the forecast period, generating a revenue uplift from these markets.

Adoption of premium platforms is far higher in the US than elsewhere, in part due to the prevalence of carrier family plans in this market. Furthermore, we feel that the fact that US carriers have embraced the family plan model also provides a strong base for further growth in this market; we believe that the number of US households paying for a digital safety solution will increase from 7.8 million in 2018 to 19.1 million by 2023.

On a regional basis, we envisage that North America will continue to account for the largest share of revenues throughout the forecast period, and these revenues will increase at an average annual rate of 24%. Growth across Asia will be somewhat more modest (CAGR 12%), but annual Asian revenues will reach more than $500 million by 2023.

However, other regions will exhibit significantly stronger growth, including:

- West Europe – CAGR 67%
- Central & East Europe – CAGR 145%
- Latin America – CAGR 153%

Additionally, there is an increasing proliferation of connected devices in a household. By upselling smart home protection solutions, carriers can extend the same controls, insights and protection to all connected devices in consumers' homes. Effectively, they achieve more holistic protection for customers, higher revenue and reduced acquisition costs. When the additional benefits, such as social responsibility and brand reputation are factored in, there is a compelling case for deployment.

5. Extending Family Safety into the Modern Digital Home

The risks that parents face with mobile devices, such as inappropriate content or screen-time, are quickly becoming prevalent in other home devices, such as tablets, laptops and portable games devices. It's becoming ever more difficult for parents to keep track and manage all devices.

Furthermore, the risks from hacking are exacerbated by the increasing number of connected devices in the home; not just smartphones, tablets and PCs, but home assistants, smart TVs, lighting systems and even refrigerators. A single weak or unprotected device can provide hackers with an entry-point to the rest of a home's network and connected devices.

Hence, any platform that can safeguard consumer devices and the home network from spyware, malware and other network attacks, as well as centrally provide family safety settings across devices, will be an attractive proposition for consumers.

A single, integrated solution that transcends the borders of a home provides parents with a simple solution that ensures family digital and, at times, physical safety whenever, wherever their children (or elders) are located.

The Avast Approach: Insight Driven

Avast is a leading consumer cybersecurity, privacy, performance and family safety solutions provider with more than 30 years' experience leading both global security and parental controls markets. Today, Avast protects hundreds of millions of users.

Avast's Threat Labs shows the quantity and sophistication of cyberattacks rising, signifying the urgency for digital family wellness and security to be a top priority. To address the challenges facing the modern, connected family, Avast has developed Avast Family Space - a parental controls solution with a robust suite of features centered around controls, insights, and location. With Family Space, parents are empowered to help shape healthy digital habits through controls and limits. Additionally, Avast deploys its AI-engine to surface actionable insights to assist parents keep up with their child's digital lives. Lastly, parents can have peace of mind knowing their loved ones are safe wherever they go.

However, digital wellness extends beyond the mobile phone. To complement Family Space, Avast has developed Avast Smart Home - a platform designed to keep all connected devices secure while extending the same mobile rules and controls to the devices in the home. Both solutions are accessible through a single companion application - parents can keep their families safe with a single, simple interface. To learn more about Smart Home, please visit www.avast.cm/mno.

Avast's successful partnerships have been built on 4 key advantages:

Cloud-based Machine Learning

Avast's proprietary machine learning engine receives a constant stream of data from millions of global endpoints enabling their technology to learn at high speeds. These insights are instantly applied across the cloud network, keeping consumers safe with the largest, up-to-date threat detection network in the world.

Massive Cybersecurity Infrastructure

Avast has a global network, with colocation at service providers allowing rapid processing of data to ensure strong throughput and minimal latency from anywhere in the world. This allows quicker updates between the network and endpoints which, in turn, contributes to our AI models and analysis by Avast Threat Labs.

Deep Experience with Leading Network Partners

For more than ten years, Avast has developed white-labeled and customized solutions for tier-1 global service providers.

Peter Hobbs, VP Global Mobile Partnerships at Avast said that: ‘Clearly, different carriers have different needs. We have capabilities to provide products which don’t require any integration; others will want deeper integration based on call and text capabilities. We have solutions that are tailor made for their particular requirements. [Carriers] want that ability to figure out what is right for their customer.’

The Avast Approach: Insight Driven

Marketing Abilities

Avast touts its ability to market alongside service providers to drive successful product acquisition and growth. With expertise in both paid and unpaid marketing, their direct and partner products have over 100 million installs annually.

Avast, in the Home

Additionally, Avast has developed Smart Home, a platform that can be easily integrated onto home routers (either directly with firmware or through a small hardware attachment). Smart Home provides consumers with a central hub to control all devices connected to the home network.

Using AI, Smart Home is able to automatically detect and distinguish all devices connected to the network. Furthermore, by monitoring data flow in real-time, the platform is able to detect unusual behaviour compared to past data and comparative data from global users. Any compromised devices are quickly quarantined and the customer notified before any harm can spread across the network.

Customers can control, monitor, and secure devices with a single companion app. Even if customers opt for both the mobile and home solutions, a single companion app allows for control of (and insights on) devices connected both inside and outside the home; the rules assigned to specific users / device profiles transcend the walls of the home.

With a proven track record protecting hundreds of millions of mobile users globally and a strong vision for the future of the smart family, Avast is one provider every operator should thoroughly evaluate. To learn more about Avast for Mobile Network Operators, visit www.avast.com/mno.