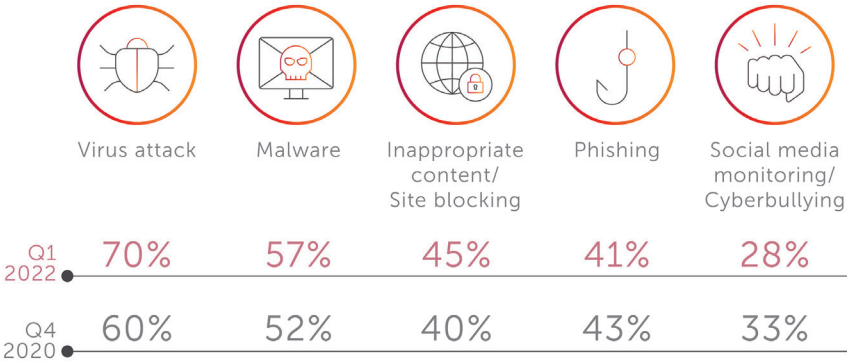
How to unravel the consumer cyber confusion

It has become an axiom that threats are on the rise. Along with the rise in threats has come a dizzying array of consumer cybersecurity solutions. As a result, consumers are paralysed and most remain unprotected, not installing a security solution on their devices. More and more internet-connected devices are also entering the home, making protection more confusing than ever. The few, technically savvy consumers that do install security solutions often need multiple solutions to cover their phones, tablets and smart devices – frequently leaving holes or overpaying for multiple point solutions.

As cyber awareness increases, consumers know that they need to be protected, but they don't know where to look. The continual increase in cyber threats creates an exceptional opportunity for communication service providers – who consumers see as a trusted advisor ►

SPONSORED ARTICLE

Phishing has also seen dramatic growth, skyrocketing during the pandemic as remote work and digitisation accelerated



Threats for which consumers have a security application installed
(Source: Allot Telco Security Trends H1 2022)

Cyber threats on the rise

This past year saw an exponential increase in threats, many targeting mobile and home devices. The **Zimperium** 2022 Global Mobile Threat Report reports that 30% of the known zero-day vulnerabilities discovered in 2021 targeted mobile devices, and there was a 466% increase in exploited zero-day vulnerabilities used in active attacks against mobile endpoints. Users can't even rely on downloading apps only from the official stores. In March 2022, it was reported that 100,000 Google Play users were infected with password-stealing malware thanks to a decoy application.

Phishing has also seen dramatic growth, skyrocketing during the pandemic as remote work and digitisation accelerated. According to **Proofpoint**'s 2022 State of the Phish report, 83% of organisations said they experienced a successful email-based phishing attack in 2021, versus 57% in 2020. Many phishing attacks specifically target mobile devices. Mobile devices also serve as an attack vector when people click on a phishing link from their mobile email app. The report also noted that 74% of organisations faced smishing attacks – attacks that took place using text/SMS messaging as the main communication vector – in 2021.

While many consumers have an anti-virus solution for their mobile phones, there are other threats such as malware, phishing and more. Consumers remain, to a great extent, unprotected.

According to the **Allot** Telco Security Trends H1 2022 report, conducted by **Coleman Parkes Research** in early 2022, among mobile subscribers that had a security app installed, 70% were protected against viruses but only 57% were protected against malware and only 41% were protected against phishing attacks.

This point is echoed by a new report from **TAG Cyber**, "Most citizens still rely on weak antivirus products that are ineffective in protecting against ransomware, identity theft and inappropriate content."

The rise of the smart home

But it's not just mobile phones that are at risk. **Statista** estimates that there are now over 300 million smart homes worldwide. The average American family has access to more than ten connected devices, such as tablets, smart TVs, smart doorbells and security cameras. The rise of the smart home, powered by home internet services, gives rise to new threats and makes managing them more complicated.

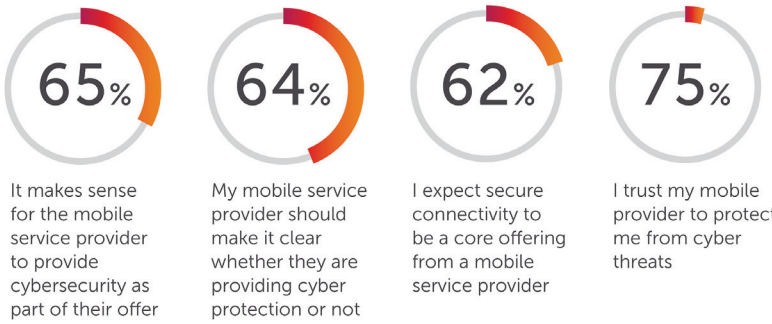
Each additional device provides more attack vectors. Besides being a victim of attacks, some attacks will even turn the victim into an attacker. Botnets, frequently used to launch distributed denial of service (DDoS) attacks, are often launched from home security cameras and connected baby monitors. Other vulnerabilities have taken over security cameras and baby monitors to allow attackers to gain access to the audio and video streams. This is surely every parent's nightmare.

Unified policy management across multiple devices

With so many devices and so many threats, it's clear that consumers need to protect themselves. But the plethora of devices and growth in threats also make it difficult to stay protected. It is cumbersome and expensive to install endpoint devices on each household mobile phone and tablet. Each device also needs its policy managed separately. It's not only phones and tablets that need protection but also the rest of the smart home – and the average household does not have the capability or technical knowledge to manage this arrangement.

Despite their confusion, consumers – and particularly Generation Z and Millennials, the oldest cohort of which are now in their 40s – are increasing their usage of security products. In **IDC**'s August 2021 Consumer Digital Life Protection Survey,[1] nearly half of the respondents in this age group stated their need for security protection increased during the pandemic and nearly an equal percentage increased their actual usage. As the pandemic has accelerated digitisation trends and made hybrid work a norm, 40% of adult respondents also stated that they will increase their usage of security tools post-pandemic. ▶

[1] IDC Analyst Brief, sponsored by Allot, Consumer Digital Life Protection: Ripe Opportunity for Communication Services Providers , doc #US48835822, February 2022



Consumers expect to receive secure internet
(Source: Allot Telco Security Trends H1 2022)

Consumers don't know how to protect themselves. According to Allot's H1 2022 Telco Security Trends report, consumers are confused

360-degree protection is a must

Traditional home security takes an ad-hoc approach and is focused on securing endpoints. It does not take a holistic, 360-degree approach. But these products don't speak to one another, and policies are fragmented across devices and services. Unified security across a consumer's entire network is the only way to ensure complete security on all their network devices.

Consumers are confused

Consumers don't know how to protect themselves. According to Allot's H1 2022 Telco Security Trends report, consumers are confused. 57% of respondents that lack a security solution don't know which to select for their devices, while 40% don't know how to select a solution.

With internet connectivity everywhere – on devices throughout the smart home, on phones, tablets, smartwatches that are both at home, at work and on the go – protection is fragmented. Solutions that only protect you at home are insufficient when you are also working partly at home, in the coffee shop, and you are taking your smart devices with you wherever you go.

It is unrealistic to expect consumers to be their own CISO. Most consumers are not technically adept and certainly cannot keep up with the ever-growing threat landscape nor manage all their internet-connected devices.

CSPs are trusted advisors

Consumers expect their communication service providers (CSPs) to advise them about how to keep their network safe. Many also expect their CSP to keep them secure. According to IDC's Consumer Digital Life Protection Survey,[1] 35% of 18-44 year old adults selected home broadband and wireless service providers as their most trusted source for home digital life protection.

According to the Allot Telco Security Trends H1 2022 report, 55% of respondents trust their mobile service provider to recommend the right security protection for them. They expect to get secure connectivity from their CSP. 58% of respondents think that their home router should be safe from threats right out of the box.

68% said that they are likely to subscribe to a service from their mobile service provider that provides security or content control on their mobile device and 65% stated that it made sense for their mobile service provider to provide cyber security as part of their offer. 62% expect secure connectivity to be a core offering from a mobile service provider.

CSPs are well positioned

While many CSPs have a well-developed managed cybersecurity business for large business consumers, there is a gap in offerings for consumers and small businesses.

Many respected industry watchers see a strong upside for CSPs. According to IDC,[1] "market demand for consumer DLP is on an upswing and will continue to grow with changing demographics (i.e., a higher percentage of the population being digital natives) and increasing awareness among consumers of the digital risks they absorb in their daily lives. Moreover, IDC[1] believes that with greater awareness, a higher percentage of consumers will explicitly take action to curb their risk. They will, in turn, seek the assurances of trusted technology providers."

Communication service providers have a strong foundation to expand their service portfolios into digital lifecycle protection and generate a dependable profit stream. TAG Cyber remarks that "The opportunity for telecom providers to offer a simple, clear package of cybersecurity protections for homes and families appears significant." IDC concurs,[1] stating, "IDC believes communication service providers have a firm foundation to expand their service portfolios into digital lifecycle protection (DLP) and generate a dependable stream of profits."

CSPs already have established customer relationships and communication channels to exploit this opportunity. They can use their billing platforms to message customers about new offerings and highlight their expertise and investment in cybersecurity – such as the number of blocks or highlight recent threats. They can also use customer online portals and applications to inform their existing subscribers about their new security offerings. ▶

[1] IDC Analyst Brief, sponsored by Allot, Consumer Digital Life Protection: Ripe Opportunity for Communication Services Providers , doc #US48835822, February 2022

CSPs engage with consumers at critical opportunities in their customers' lives and are well-positioned to build brand loyalty. This includes household moves, mobile device purchases and service agreement renewals, as well as service-related issues. One of the critical challenges with marketing and selling any new service is reaching a potential user at exactly the right time. However, the CSP-consumer lifecycle is perfectly positioned to take advantage of multiple touchpoints to educate and grab subscribers when they are ready to buy.

IDC[1] writes that "leveraging their network infrastructure and home broadband routers as service delivery platforms, communication service providers have the means and motivation to expand their DLP offerings from which to grow average revenue per user (ARPU), carve out competitive differentiation, and strengthen customer loyalty." By partnering with a security provider, CSPs can take advantage of the significant potential. This is due to:

1. **Reducing churn** – 80% of respondents in the Allot H1 2022 survey said that they would probably or definitely switch to a new provider if they offered a security service. No, they're not bluffing – 42% of respondents switched service providers within the past three years.
2. **Increasing differentiation** – 64% of respondents said that service providers should make it clear whether they are providing cyber protection or not.
3. **Incremental revenue potential** – Partnering with a provider that operates on a revenue-share model, CSPs can reduce their initial risk, while taking advantage of significant upside potential.

TAG Cyber has created a sample business case for a small telecoms operator in the United States, noting that even small providers can increase their revenue by hundreds of millions of dollars annually after ramp-up. This can be done with a low initial investment from CSPs by partnering with a provider that offers zero or low-front costs, but rather is willing to share the risk with a revenue share model.

CSPs already have established customer relationships and communication channels to exploit this opportunity

Allot's SECaaS Solution

Allot is a leading vendor providing security-as-a-service to CSPs. Allot is a well-known and established player in the CSP market, providing advanced telecoms solutions that serve over one billion subscribers worldwide. Allot provides security-as-a-service solutions to CSPs, achieving up to 50% penetration with some service providers, and currently serving over 20 million subscribers globally. Allot is seeing increased interest in network-based cybersecurity solutions. CSPs are choosing Allot to provide their security services, having signed 11 deals in 2021.

These solutions offer zero-touch 360-degree protection, securing all devices through the home and mobile network, as well as providing endpoint protection when traveling off the network. No customer effort is required to provision security. No matter where the devices are located, security policies are centrally managed through a unified cloud-based management console, with no need for complex configurations across multiple devices.

Allot Secure unifies core-network-based security with endpoint and customer premise equipment-based (CPE) based security enabling CSPs to deliver branded, security services to the mass market. Allot Secure also protects the network user plane, detecting and mitigating both inbound and outbound DDoS threats. It also prevents connected IoT devices from launching malicious, reputation-damaging traffic through your network.

Customers are kept informed on how you've protected them, helping to achieve an ongoing perception of value and high customer satisfaction.

To learn more about Allot's security services for CSPs, contact us at **bspielman@allot.com**

allot

www.allot.com

[1] IDC Analyst Brief, sponsored by Allot, Consumer Digital Life Protection: Ripe Opportunity for Communication Services Providers , doc #US48835822, February 2022