Global Consumer Security Survey

Telco Security Trends

December 2020

Table of Contents

Introduction

H2 2020 began just a few months into the COVID-19 global health crisis, as governments, businesses and individuals around the world were adjusting to an uncertain new reality that fundamentally altered every aspect of our lives. By June, the upheaval had spawned a few clear trends that would define the 'new normal' of life alongside the pandemic. Road congestion, oil consumption and air pollution plummeted as people were confined to their homes and unable to travel. Internet use skyrocketed as people spent more time online keeping up with news, consuming entertainment, communicating with loved ones and connecting to work from home (WFH). The OECD reports that since the start of the COVID-19 crisis, "demand for broadband communication services has soared, with some operators experiencing as much as a 60% increase in Internet traffic compared to before the crisis."

Fear and uncertainty, combined with increased internet use, also provided the perfect conditions for cybercrime. According to the Interpol Covid-19 Cybercrime Analysis Report – August 2020, member countries have experienced large increases in Online Scams and Phishing, Disruptive Malware (Ransomware and DDoS) and Data Harvesting Malware. Cybercriminals reacted quickly to the crisis, registering malicious domains with health and medical names.

In the first two months, reports to Interpol skyrocketed:

569% growth in malicious domain registrations, including malware and phishing

788% growth in high-risk domain registrations

Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."

Jürgen Stock,
INTERPOL Secretary General

Interpol predicts a further increase in cybercrime is highly likely and vulnerabilities created by work-from-home will continue to be exploited by increasingly sophisticated attack methods. The organization also expects coronavirus-themed online scams and Phishing campaigns to continue to proliferate. A surge of business email attacks is also expected. When the long awaited Covid-19 vaccine is finally available, it is highly probable we will see another dramatic spike in Phishing campaigns related to medical products and network intrusion and cyberattacks to steal data.

Against this dramatic backdrop, in June 2020 Allot, together with London-based Coleman Parkes Research, began an extensive global survey of consumer cybersecurity practices and attititudes. Over the next four months 11,400 consumers in North America, LATAM, APAC and EMEA were surveyed. The research questions measured attitudes toward online security, to learn how consumers are securing themselves online, what's preventing them from implementing effective solutions and what role communication service providers need to play in protecting their users. The results of these surveys are enlightening, including clearly pointing to the fact that consumers feel strongly that CSPs should be providing cybersecurity services, they are willing to pay an additional monthly fee for such services, and many would be willing to switch providers to be on a more secure network.

Key Research Questions

As the cyberthreat landscape grows more menacing and pervasive, it is important for CSPs and network security solution providers to have a deep, thorough understanding into the mindset and behaviors of consumers. Only when we know consumers well, can we then identify unmet needs and deliver compelling security solutions they will be happy to pay for.

- **How concerned are customers about cybersecurity? Which cyberthreats are the greatest concern?**
- **Which security solutions are customers already using?**
- **Who do customers believe is responsible for security protection? Device manufacturers, service Providers or 3rd party endpoint software?**
- **Do consumers trust their CSP to provide security protection?**
- **Do parents want better parental control solutions? If so, which features?**
- **Would advertising a clear security service or 'most secure network' prompt people to switch providers?**
- **Are consumers willing to pay for CSP-provided security protection and parental controls?**

Cyberthreats: The Great Equalizer

When conducting global research of 11,400 consumers in 13 countries, you naturally expect results to show quite a bit of variation between the regions. Surely the attitudes, habits and consumer behaviors will vary significantly from country to country. Surprisingly, as all the data are tallied and compared, the most striking observation is the similarity among all regions. It seems that the internet and cyberthreats are truly universal. People and businesses around the globe show similar patterns of online behavior and concern and response to growing cyberthreats.

Consumers are Concerned

Your consumers are very concerned about security risks. When asked which cyberthreats concerned them the most they listed; viruses (**62%**), loss of sensitive data (**59%**), loss of privacy (**59%**), Phishing (**51%**), hacking (**51%**), and cyberbullying (**44%**).

51%

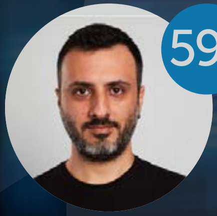
Hacking

44%

Cyber bullying

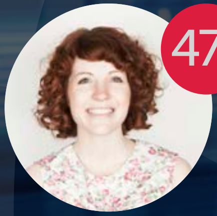
62%

Viruses infecting my devices



59%

Loss of sensitive data



47%

Children's exposure to cyber threats

43%

Ransomware

59%

Loss of privacy

51%

Phishing attacks

45%

Spamming

38%

Excessive use of the device by your children/ children in general

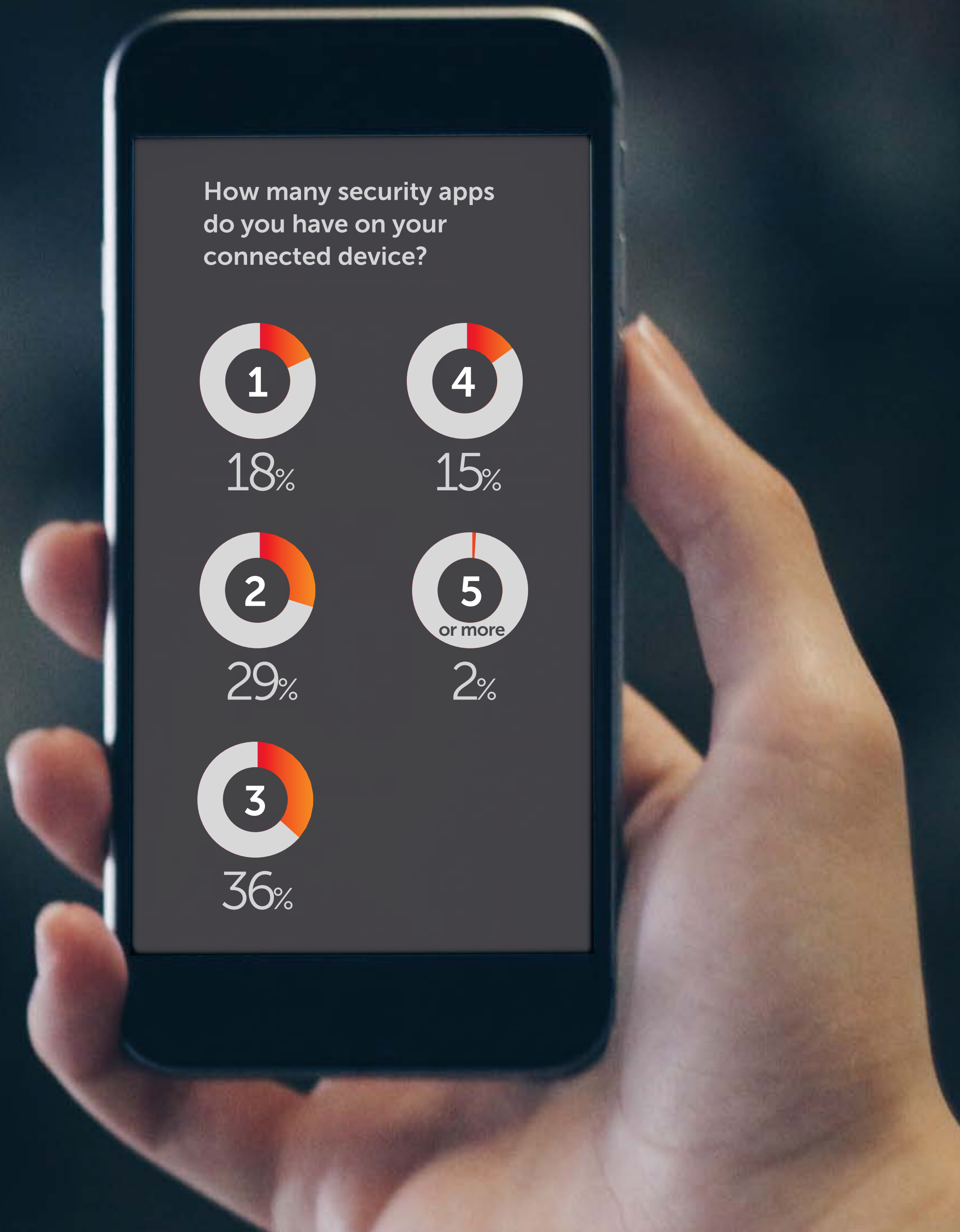
Trying to Defend Themselves

CSP customers are aware and concerned about cyberthreats. They are already taking action to defend themselves. The majority of respondents (**89%**) had at least one form of security on their connected device. Globally, an average of **60%** reported having an antivirus solution and **52%** anti-malware. Only **43%** of users reported having a Phishing protection solution installed. This is particularly concerning, considering Phishing is by far the most pervasive form of cyberattack today.

11% have no security protection whatsoever.

There is a large variety in the types of threats users are trying to defend themselves against. Of those who reported having at least one security app on their device, **82%** had 2 or more solutions, showing the need to piece together a complete coverage from multiple 3rd party vendors. All this time, effort and money is already being spent on non-CSP security and parental control solutions.

How many security apps do you have on your connected device?



Do you have an app on your mobile device to protect against the following threats?

60%	52%	43%	40%	33%	11%
Virus	Malware	Phishing	Inappropriate content	Social media monitoring	None of the above

Barriers to Comprehensive Security

How can we explain the wide gap between high customer awareness and concern and low implementation of security solutions? This next question delved deeper into understanding all the nuanced factors preventing customers from consistently implementing complete security solutions across all connected devices. Amongst those consumers who did not have any security solution, over a third said the reason was because it was too costly. Consumers in North America were most sensitive to price. But many are simply confused about the need and bewildered by the choices available. Perhaps this shouldn't come as a surprise; most of the population aren't IT security professionals.

It is worth noting that users in APAC are most likely to think cybersecurity isn't necessary (**45%**), perhaps reflecting a strong regulatory environment where citizens feel protected. In contrast, North Americans show a particularly troublesome trinity of lacking the technical know-how (**53%**), impatience for installation and maintenance (**41%**) and by far the most cost sensitive (**60%**).

What prevents you from investing in securing your Internet connected devices?

	APAC	EMEA	LATAM	NA	Global
Too costly	21%	34%	28%	**60%**	**35%**
Do not know which to choose	17%	33%	29%	36%	**31%**
Don't think it's necessary	**45%**	29%	25%	31%	**30%**
Do not know how to do it	20%	27%	28%	**53%**	**29%**
Too much hassle to install and maintain	22%	28%	22%	**41%**	**28%**
I would not know where to look for a solution	27%	26%	23%	39%	**27%**
I expected it to be on the devices	20%	26%	32%	30%	**27%**
Worry about adding apps	19%	25%	25%	38%	**26%**
I trust my child so do not need it	7%	13%	12%	23%	**13%**

Who is Responsible?

Another factor preventing consumers from implementing effective cybersecurity solutions may be confusion about whose responsibility it is. Responses to the question, “Who do you think should provide cybersecurity protection for your Internet connected devices?”, reveal that many believe that the device manufacturer (**28%**) or the CSP (**29%**) is responsible. Only **23%** believe they should download an app themselves. An additional **20%** believe the app should be preinstalled by either the device manufacturer or CSP.

This reflects a pervasive culture of consumer safety, in which people assume that if the device is sold by a reputable brand, it must be safe for use. This also explains why so many of your customers believe you, a government sanctioned communications provider, are responsible for delivering safe internet access.

Who should provide cyber security protection for your connected devices?

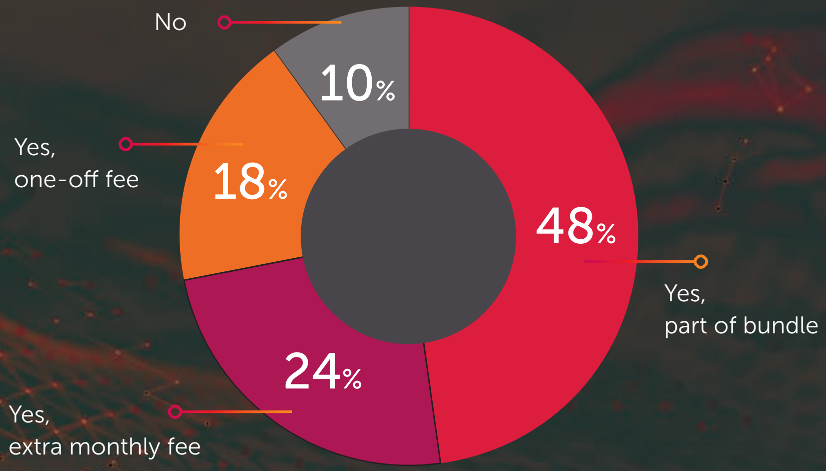
	APAC	EMEA	LATAM	NA	Global
The device manufacturer (e.g., Apple, Samsung, etc.)	26%	28%	31%	31%	**28%**
Your service provider	31%	28%	32%	28%	**29%**
An app pre-installed by manufacturer or CSP	19%	20%	18%	22%	**20%**
You need to download an app yourself	24%	24%	20%	18%	**23%**

77%

77% believe they are not responsible for securing their connected devices

Consumers Trust CSPs to Provide Security

The results show that even though historically CSPs provide connectivity, not security, consumers also consider them to potentially be a trusted provider of cybersecurity protection. When asked, “Do you think that the service provider should provide you with a security solution?”, **90%** answered ‘yes’. **48%** of those said security should be included as part of a bundle, **24%** said it should be an extra monthly fee, and **18%** said it should be available for a one-time fee.



Do you think that the service provider should provide you with a security solution?

	APAC	EMEA	LATAM	NA	Global
Yes, part of bundle	36%	52%	56%	49%	**48%**
Yes, extra monthly fee	27%	24%	23%	24%	**24%**
Yes, one-off fee	26%	14%	18%	18%	**18%**
No	11%	11%	4%	9%	**10%**

90%

90% of consumers think the CSP should provide a security solution either as a part of the bundle or for a monthly or one-time fee.

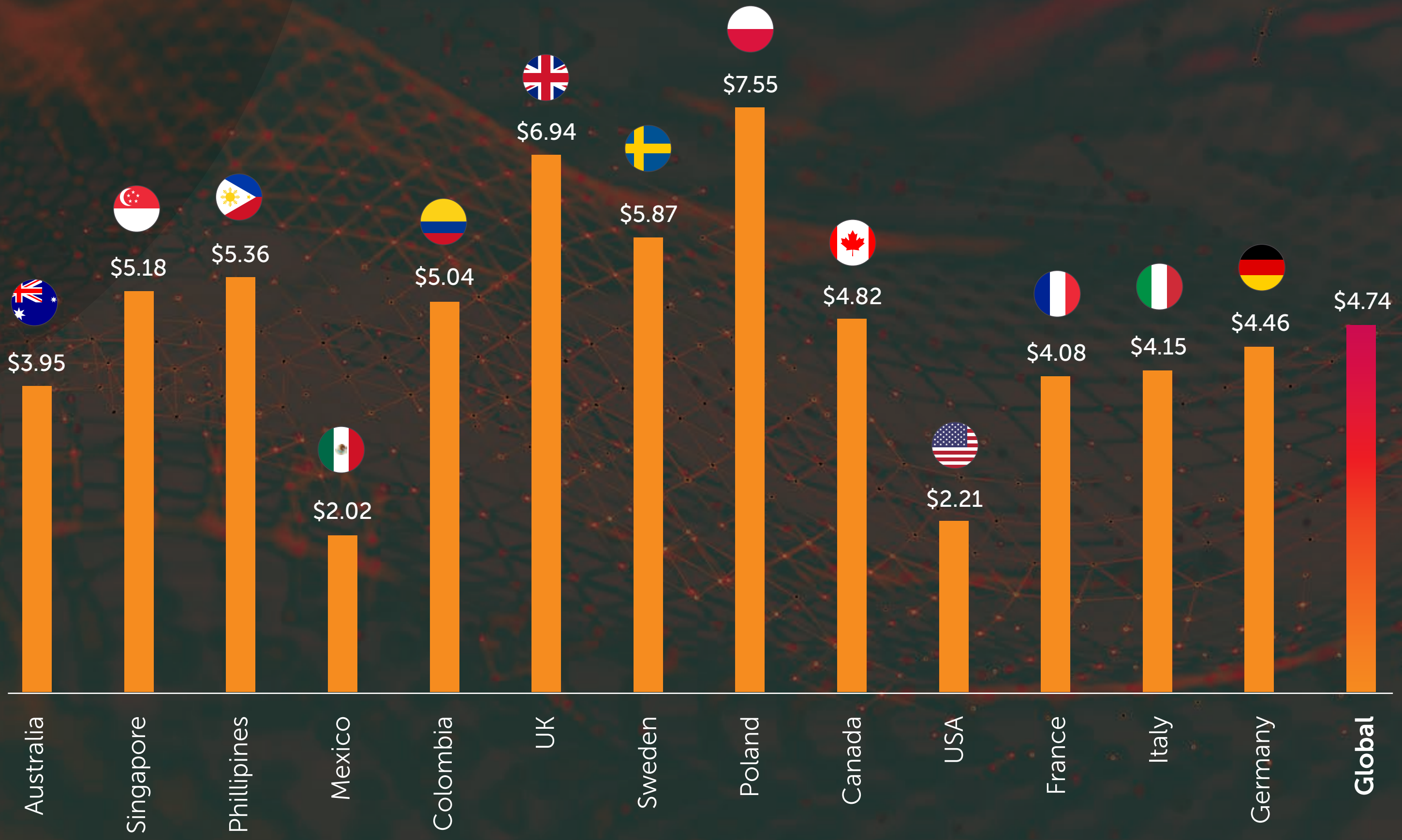
Willing to Pay ~$5 Extra Per Month

Consumers don't just expect CSPs to provide security, they are willing to pay for it. This shouldn't come as a surprise, since globally **42%** of your customers are already paying a 3rd party provider directly for some kind of security program or app.

CSP-provided network-based cybersecurity offers your customers better protection, with none of the hassle, at a fraction of the cost.

The average additional price people are willing to pay their service provider for a network-based security solution is **$4.74**. Consumers in Poland (**$7.55**) and the UK (**$6.94**) are willing to pay the highest additional monthly fee, while consumers in Mexico (**$2.02**) and the US (**$2.21**) are the most price sensitive. The amount people are willing to pay does not at all appear aligned with GDP. Two factors that likely influence this figure are how at risk they feel and their perception of current service provider costs and value.

Average amount consumers are willing to pay per month for a CSP provided network-based security solution



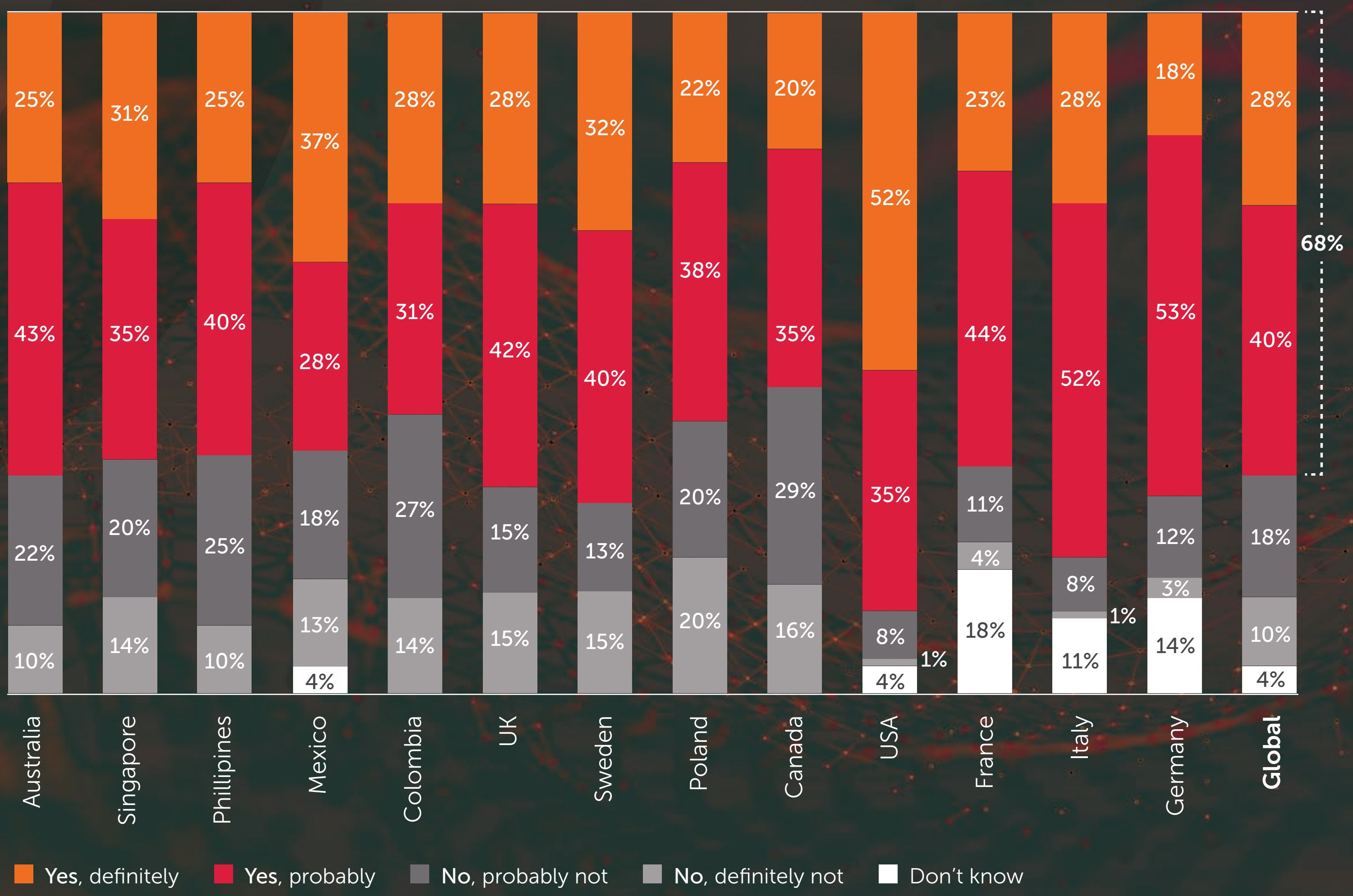
Willing to Switch to More Secure Provider

Cybersecurity is so important to consumers, **68%** said they would switch providers to be on a more secure network. **28%** said they would definitely switch. An additional **40%** said they are likely to switch because security is quite important to them.

Customers in the US were more likely to say they would definitely switch (**52%**), followed by Mexico (**37%**) and Sweden (**32%**). The customers least likely to switch providers who said they would definitely **not** switch were in Poland (**20%**), Canada (**16%**) and the UK (**16%**).

7 out of 10 would switch to a more secure provider.

Would you switch provider to have better security?

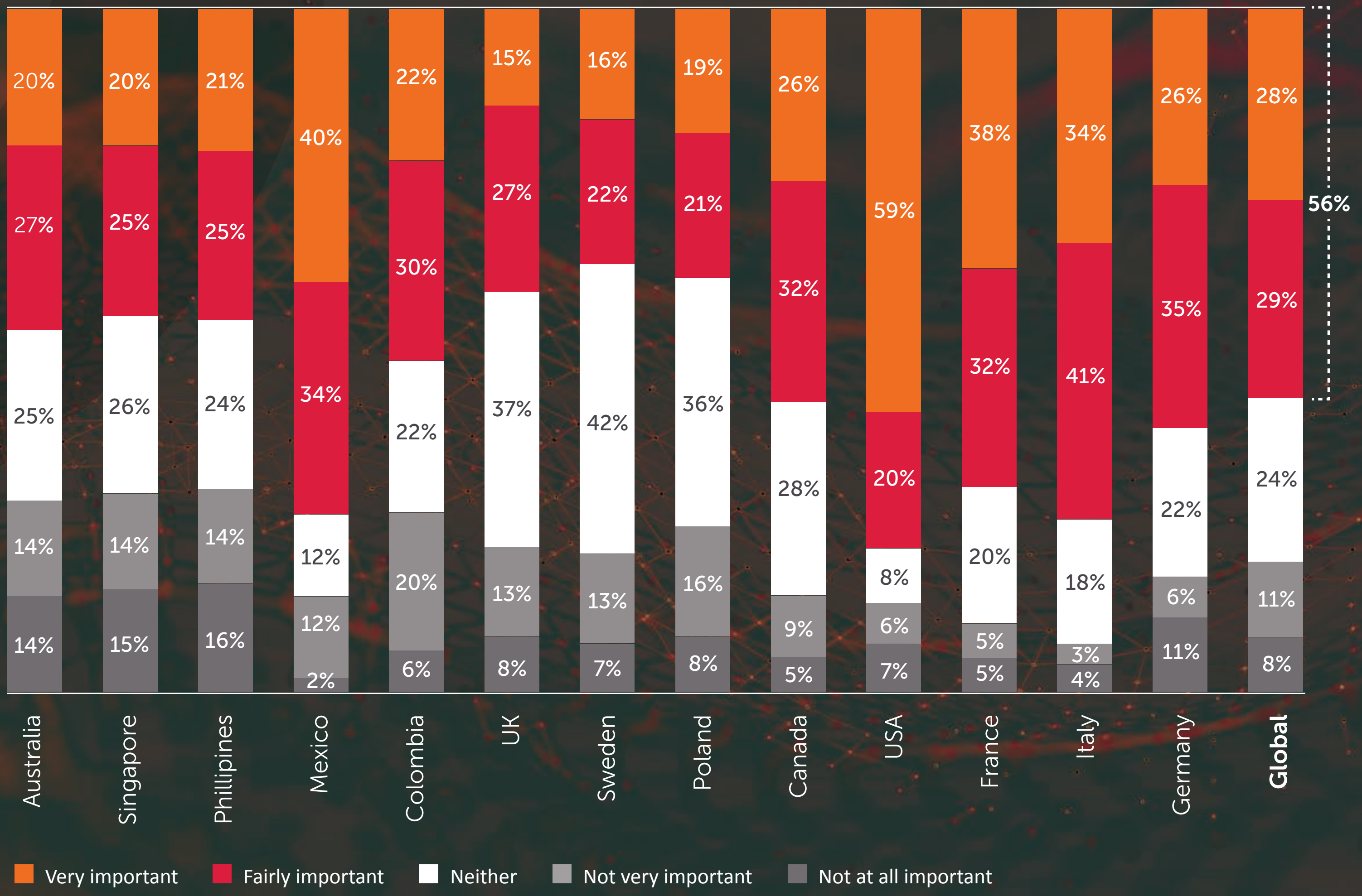


Families & Parental Control

Families with school-age children are a very important target segment for both network-based security protection and parental controls. It comes as no surprise that parents are very concerned about protecting children and therefore extremely security conscience. They are also the most willing to spend on security solutions. Parents who spend hundreds of dollars on Wi-Fi connected nanny-cams and purchase tablets and smartphones for young children, are highly likely to spend a few extra dollars a month for comprehensive hassle-free security, especially if it can also include content-filtering and parental controls to keep their children safe online.

Adding parental control expands the available market considerably as 56% of all consumers said parental controls are important.

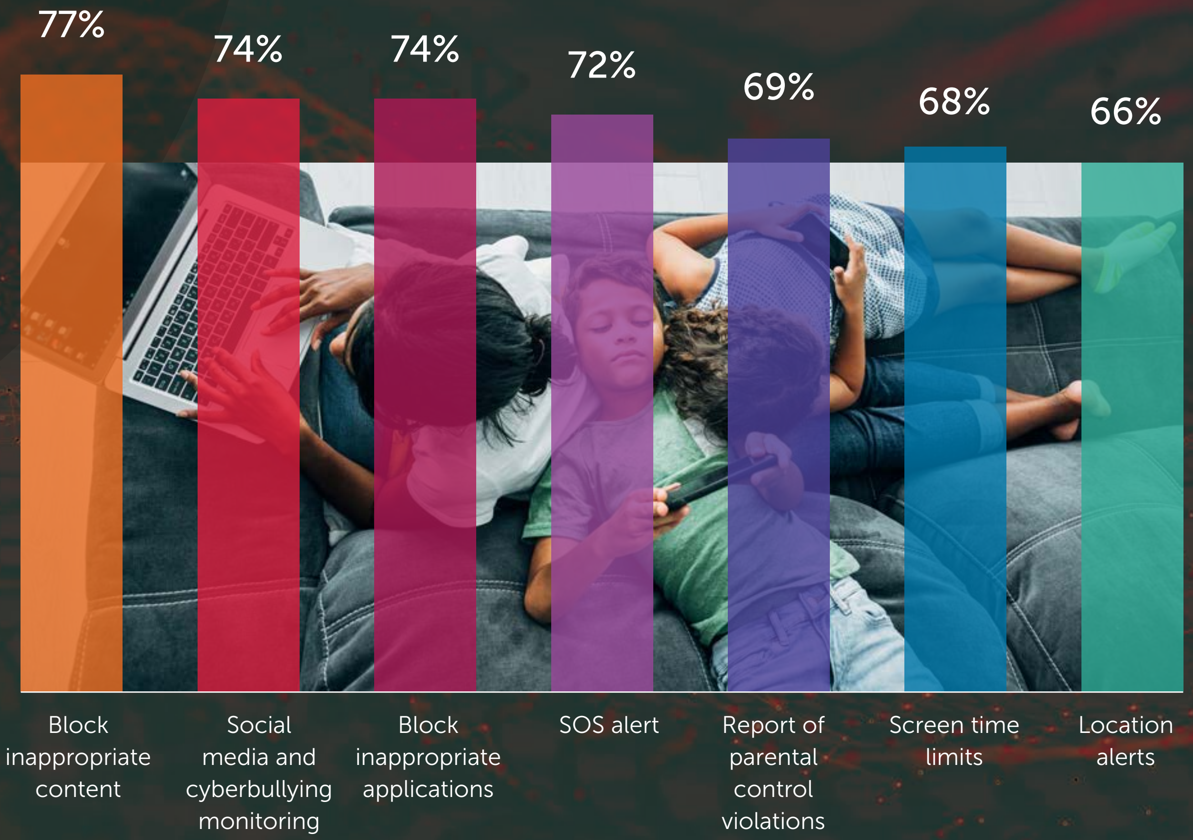
How important is a parental control service to you?



Parental Control Features

The broad term 'parental control' includes many different kinds of services and leaves room for ambiguity. To pinpoint exactly which features are most important we asked customers to choose the top five parental control features which are most important to them.

Which parental control features are most important?



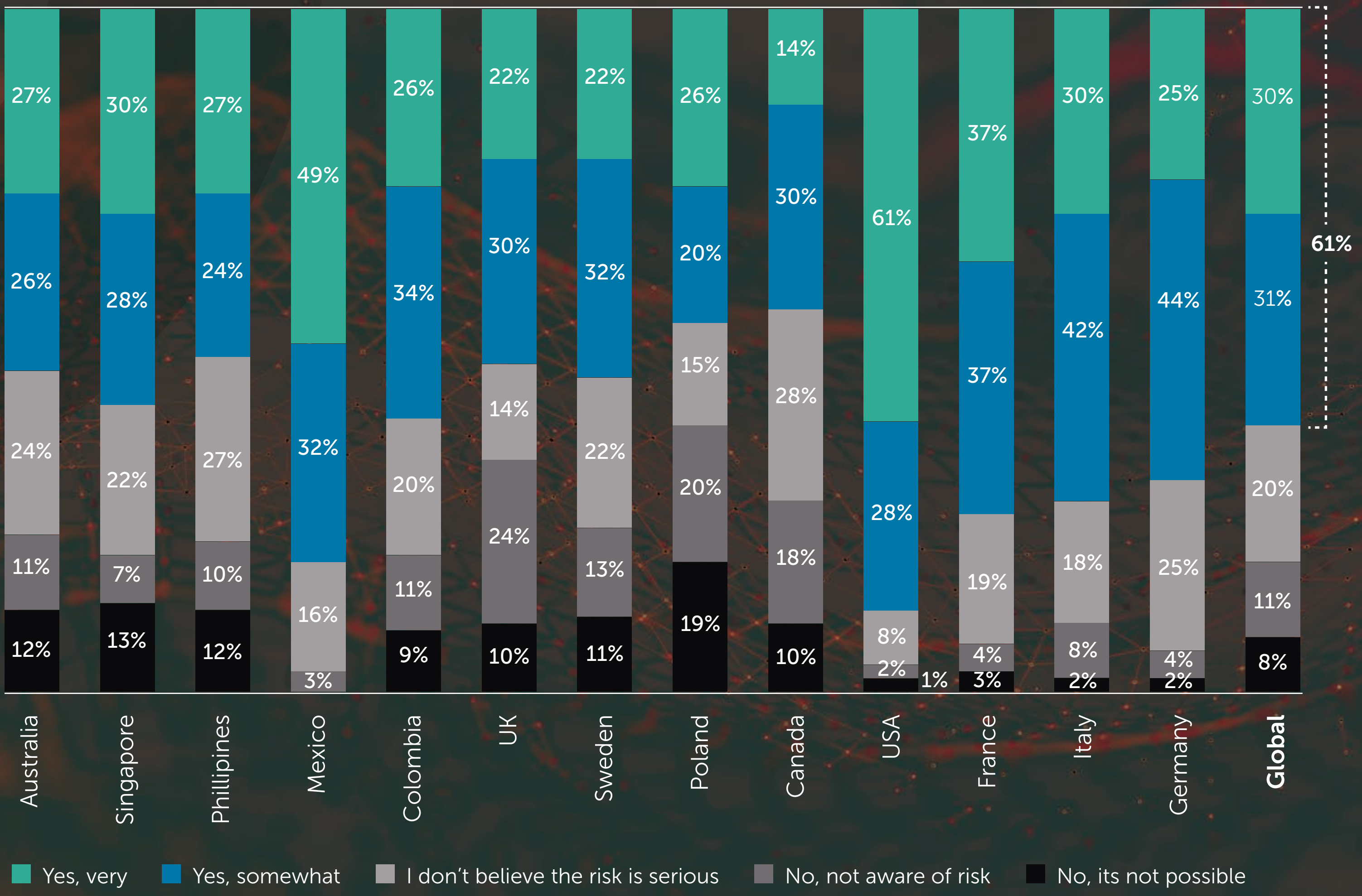
Connected Home Invasion

Our homes are rapidly being upgraded with smart TVs, home security systems, smart kitchens, smart energy and smart lighting. IDC predicts worldwide smart home device shipments will grow at an annual rate of **14%** from 854 million units in 2020 to more than 1.4 billion units in 2024.

But these 'smart' devices use our home network as a gateway to the Internet, sending and receiving data, and being upgraded via software updates. This increases the number of devices we own that might be the entry point for a cybersecurity breach, and the variety of ways malicious software could penetrate our daily lives.

What is worrying is that while consumers adopt a more digital lifestyle, they do not complement it with a digital security effort at nearly the same level of enthusiasm. At the end of 2019, only **36%** of U.S households were using paid cybersecurity, identity or privacy products (with Antivirus leading the pack, leaving far behind it other defenses for more modern threats).

Are you concerned that the microphones and cameras in 'smart' devices, can be hacked and used to spy on you and your family?

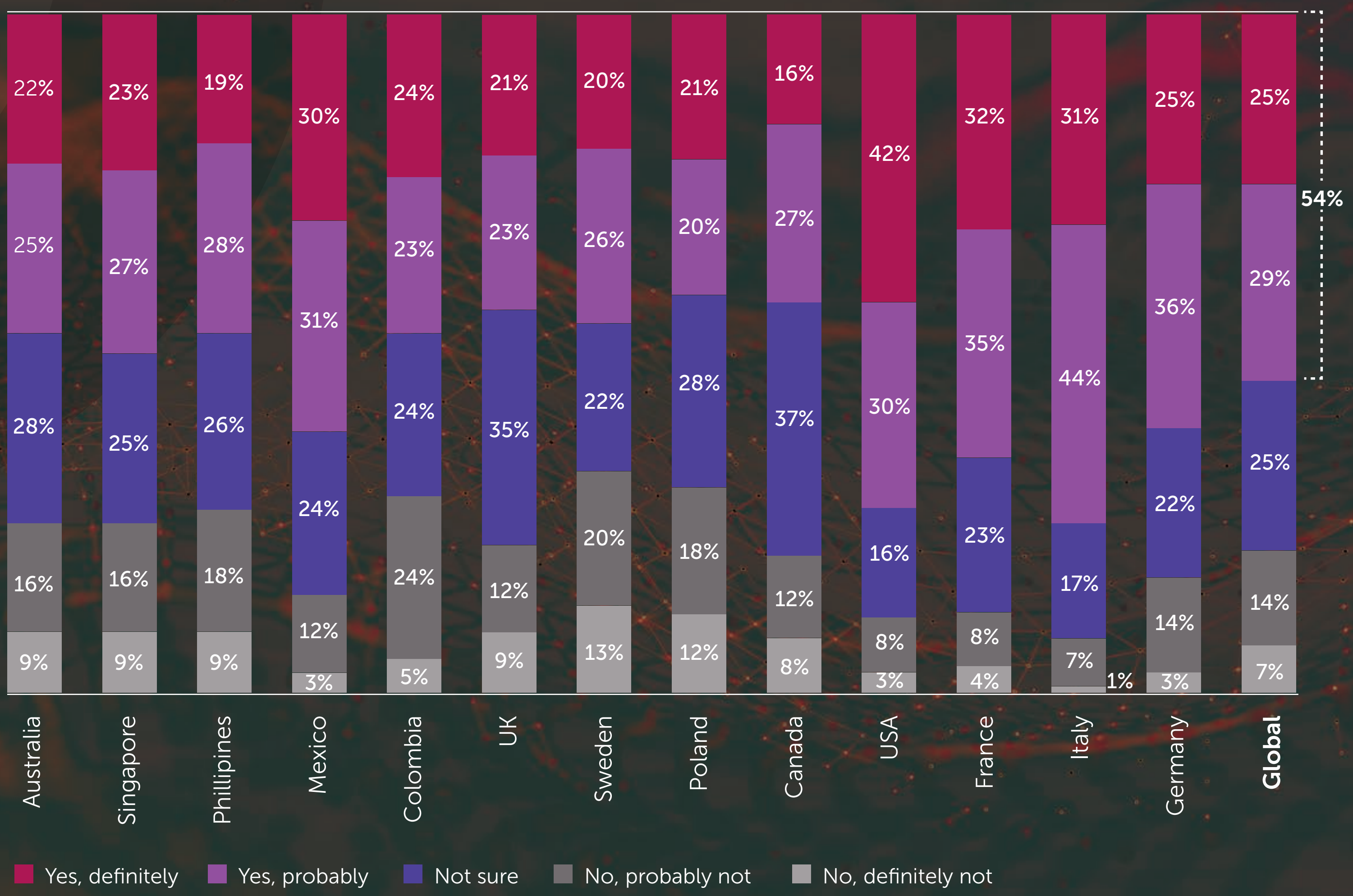


Covid-19 Impact

Cybercriminals were quick to exploit the Covid-19 environment. As businesses had to close their doors and offices, employees shifted to work-from-home and people dramatically increased the time spent online staying up-to-date with news, consuming online entertainment and shifting to ecommerce. This increased online activity alone would be expected to increase the level of risk for every Internet user. Add on top of that, increased activity of cybercriminals and specific attacks that exploit people's fear of Covid-19, and the risk is substantial.

54% think the Coronavirus crisis has also increased risk of cyberthreats

Do you think there is added risk of security threats in the Coronavirus era?



Cybersecurity Global Opportunity

Facing both growing threats and substantial barriers to implementing protections, CSPs and their customers have serious cause for concern. The good news is CSPs are perfectly positioned to capture this market by delivering a comprehensive zero-touch solution through the network at a low cost. You already own the pipeline and have access to a large customer base. CSPs can deliver a zero-touch network-based clientless security solution that protects all devices. The network is the best way to deliver security to consumers for the following reasons:

- **For broadband, the CPE is already in place and is the first point of entry to all connected devices in the household**
- **For mobile operators, all your subscribers' data traffic goes through the network, making it an ideal place for detecting and mitigating cyberattacks**
- **No-touch service is automatically activated without downloading software**
- **Access to large customer base who trusts, and even expects, the service provider to offer security protection**
- **Very price competitive. No more than a few dollars per month**
- **Strong demand from families with young children; CPSs can also offer content filtering/parental controls**
- **Strengthen brand and increase NPS**

Click to learn:
How Service Providers Offer Customers Network-based Cybersecurity Protection
or watch this video:
How Allot NetworkSecure Works

allot Secure
Cybersecurity Protection for the Mass Market

Allot Secure is a security service delivery platform designed for CSPs that centrally manages and unifies multilayer, multivendor security. It unifies network-based security, home and business gateway security and security clients into your own branded security service. Allot Secure delivers a seamless customer experience through a single interface for policy setting, reporting, and event handling. Allot Secure is comprised of the following security components:

NetworkSecure: A network-based security layer that enables CSPs to deliver secure web services and parental control. Frictionless onboarding and mass activation produce high adoption rates while securing all network-connected devices.

HomeSecure: Security for home IoT, smart appliances, and home offices. Integrates existing CPE with the addition of a thin client that provides home network visibility and security with minimal impact on CPU and memory.

BusinessSecure: Simple & reliable network security for SMBs. External and internal attacks effectively blocked. Unmatched security and visibility into the business network.

EndpointSecure: Integrates and centrally manages 3rd party endpoint security clients to provide a seamless customer experience and persistent security for customers who switch between the operator's network and Wi-Fi in public locations.

IoTSecure: IoT security and value-added service for enterprise customers. Provides increased operational efficiency and IoT service monetization, securing IoT services and CSP infrastructure.

DDoS Secure: The only inline bi-directional DDoS mitigation system designed for carrier networks with Tera-bit scale. Automatically removes DDoS attack traffic within seconds while maintaining maximum QoE for all legitimate network services.

About Allot

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and security solutions for service providers and enterprises worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-based security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our industry-leading network-based security as a service solution has achieved over 50% penetration with some service providers and is already used by over 20 million subscribers globally. For more information, visit www.allot.com or Contact Us

allot
See. Control. Secure