allot
See. Control. Secure.

Position Paper

Switch to Security: Consumer & SMB Security Survey – LATAM 2020

September 2020

Table of Contents

Introduction

During June and July of 2020, Allot partnered with Coleman Parkes Research Group to survey 1400 LATAM (Columbia 700, Mexico 700) mobile subscribers and 600 SMBs (300 Columbia, 300 Mexico) to assess their cybersecurity awareness and behavior. Overall, mobile customers across the region showed high levels of awareness and concern about cybersecurity threats. Yet a general uncertainty about exactly which steps they should be taking to protect themselves prevailed, suggesting the market is far from mature. These results are in line with findings of a US mobile consumers survey published by Allot in July 2020.

A large proportion believe that their CSP should provide protection against online threats and expressed a willingness to pay an additional monthly fee for an easy-to-use solution that protects all their connected devices at home and on the go. 60% of LATAM consumers said security was so important to them, they would 'definitely' or 'probably' switch to a provider with a clear security offering.

6 out of 10 LATAM consumer & SMB customers would switch to a provider with a clear security offering.

Consumer Awareness & Concerns

Consumers are clearly very concerned about cybersecurity. The abundance of frightening press coverage about all types of threats have had a strong effect on the general public.

The survey showed that 45% have been, or suspect they have been, the victim of a cyberattack themselves in the last 12 months. An additional 24% know someone personally who was a victim in that time frame.

In addition, parents with school-aged children are also highly concerned about protecting devices used by children from malware and viruses and would like parental control features.

Threat is Everywhere

82% of mobile consumers worry about their device getting hacked while connected to the mobile network

Mobile consumers assess their own cyber risk to be high, no matter where they are or how they are connecting to the internet. When asked to rank their top concerns in relation to hacked devices, 82% cited getting their mobile hacked while connected to the mobile network, 83% said their mobile being hacked via home router, 84% via connected home devices, and 84% worry about their mobile getting hacked while connected to public Wi-Fi. When we asked parents specifically about their children's devices getting hacked on public Wi-Fi only 32% listed it among their top concerns; likely due to younger children not often connecting to public hotspots and their phones not containing bank or credit card data, so the potential damage is perceived as lower.

Home, Mobile and Public Wi-Fi

When asked explicitly where, or via which internet connections, consumers feel they most need security protection, the highest level of concern was for connection via the mobile network at home (40%), followed by the home router (32%), and finally public Wi-Fi (28%).

Security Threats in the COVID-19 Era

The COVID-19 crisis has contributed to a strong surge in cybercriminal activity. More time spent online and more people working from home and accessing business assets over unsecured connections is enough to increase the risk. Add to that the psychological effects of prolonged fear and uncertainty, and you have very fertile soil for all types of cyberattacks.

The global health crisis of the past few months has also heightened the perceived threat among mobile customers. When asked if they think the coronavirus era has brought with it an added cybersecurity risk, 47% answered 'yes', 49% were not sure, and 4% did not think the situation has changed.

47% of consumers think the coronavirus has increased cyberthreats

COVID-19 has had a powerful effect on the entire population and has made them more aware of all kinds of threats and much more willing to take serious steps to protect themselves. Since April 2020, Allot Secure CSP customers around the world have experienced double-digit growth in their cybersecurity service adoption as customers become more concerned about cyber risks and turn to their CSP to provide trusted solutions.

Partial, Inconsistent Solutions

Consumers are not just concerned; they are ready to take action. Roughly half of survey respondents stated they have at least one type of security solution on at least one of their devices. 53% have an antivirus solution, 50% have phishing protection, 53% block inappropriate content, and 46% have implemented a social media monitoring solution. On average, 51% of LATAM mobile consumers have an anti-malware solution on their device, with a 5% difference between the countries; Columbia 54% and Mexico 49%.

On the one hand, this shows that the consumer market is motivated to acquire cybersecurity protection. But it also paints a picture of incomplete and inconsistent solutions, where each user is on their own trying to figure out how to protect their devices. They have implemented partial solutions that cannot provide comprehensive protection against all threats, on all devices, no matter where or how they connect to the internet.

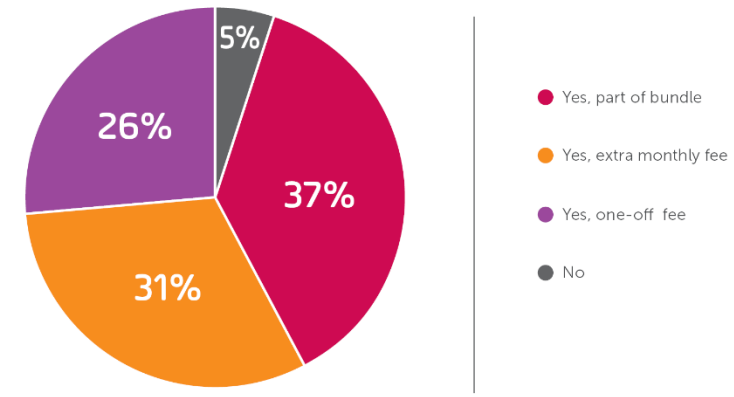
Consumers seem to take a 'set it and forget it' approach wherein they have a singular instance of concern and seek out a single solution, implement it, and then don't want to spend any further time or energy investigating additional solutions or updating the one they have.

Consumers Trust CSPs to Provide Security

95% said that their CSP should provide security solution

Perhaps most interestingly, though not surprisingly, 95% of respondents in this survey said that their service provider should provide security solutions. This is a strong vote of confidence that customers trust the provider to deliver quality protection. 37% of those subscribers believe security should be provided as part of the bundle, showing many customers also *expect* the CSP to provide security solutions. Overall, the responses show strong preference for CSPs to take responsibility for securing the entire home and all devices in a simple manner that requires little or no technical involvement from the consumer. They want to leave security in the trusted, capable hands of the CSP.

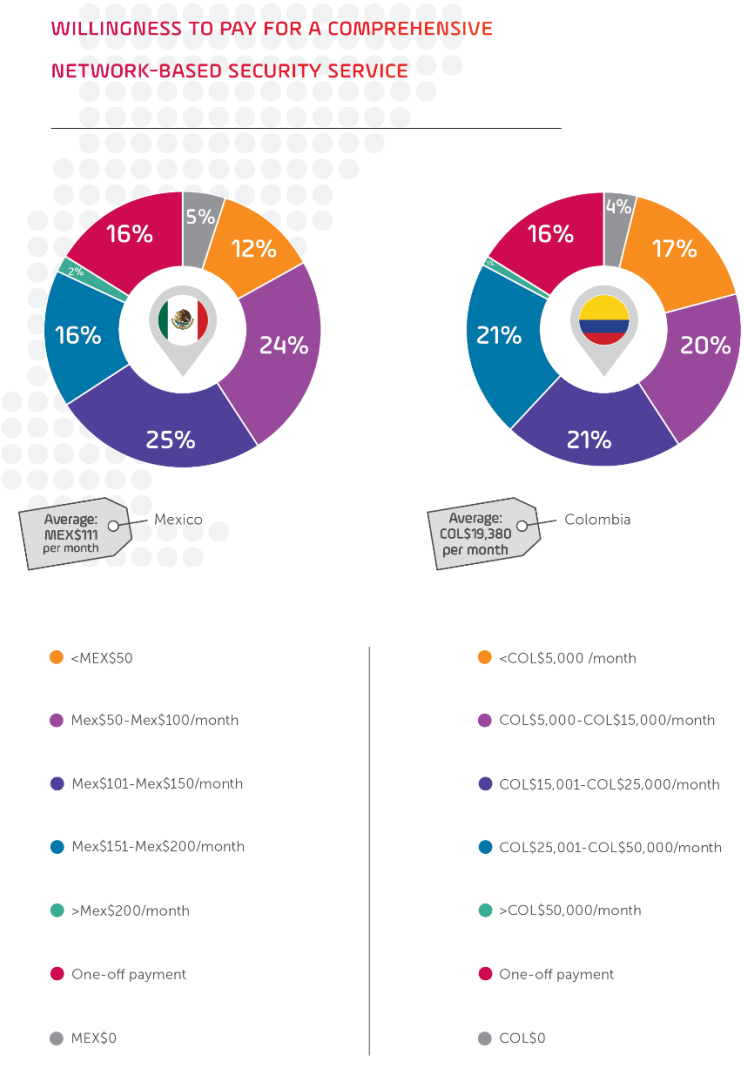
SHOULD YOUR CSP PROVIDE A SECURITY SOLUTION?



Willingness to Pay

66% of LATAM parents are willing to pay their CSP an additional $4.50 USD or more for parental control features.

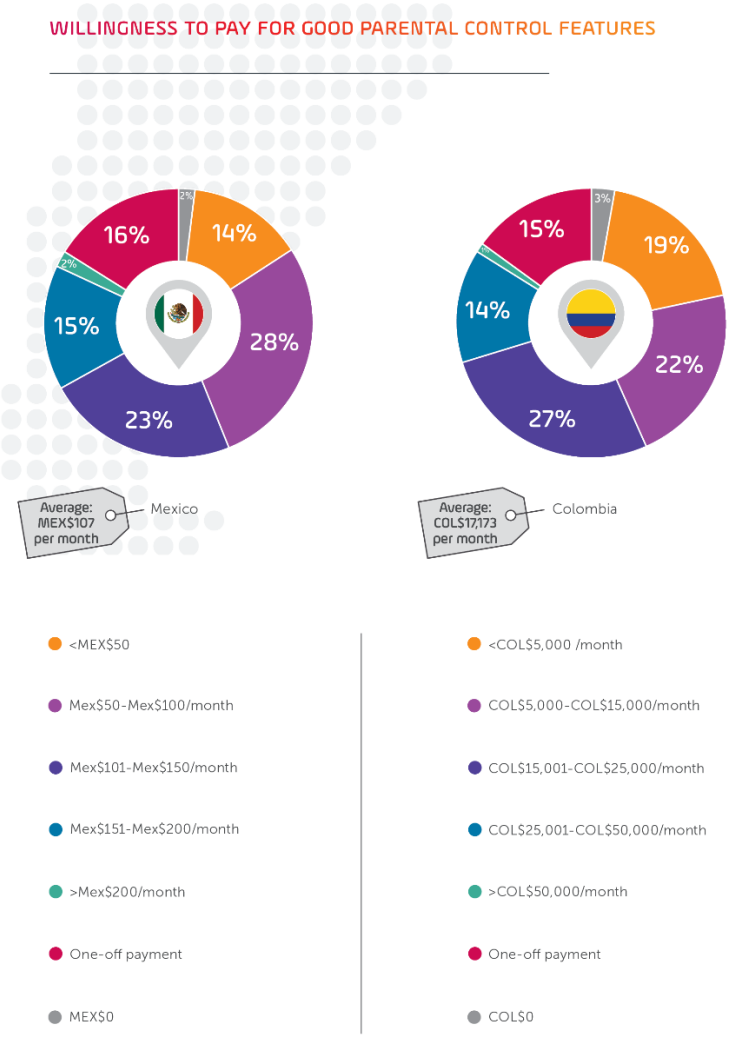
Taking it one step further, we asked mobile subscribers who had at least one security tool already installed, how much they would be willing to pay for a comprehensive, hassle-free security solution provided by their mobile carrier. The responses show a large percentage are willing to pay for such a solution. 65% of Mexican subscribers are willing to pay an additional MEX$50-200; average **MEX$111 ($5.06 USD)** per month. 62% of Columbian subscribers are willing to pay an additional COL$5,000 or more; average **COL$19,380 ($5.00 USD)** per month.



Parental Concerns & Controls

Naturally, parents in LATAM are highly concerned about their children's activity and safety online. 46% said that parental controls to monitor and protect their children online are important to them. They very clearly articulated the type of parental control features they desire, notably, limiting screen time (43%), location updates (43%), social media monitoring and cyberbullying protection (44%).

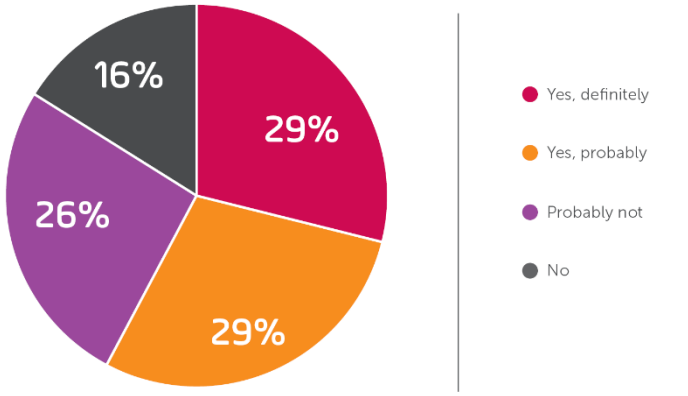
68% of Mexican parents are willing to pay their CSP an additional Mex$50-200; average **MEX$107 ($4.88USD)** on top of their current monthly fee for parental control features. **64%** of Columbian parents are willing to pay their CSP an additional COL$5,000-50,000; average **COL$17,173 ($4.45USD)** on top of their current monthly fee for parental control features.



SMBs Seek External Security Provider

SMBs across LATAM have adopted digitization to power their businesses, but this reliance on information technology, mobility, IoT and the internet has also increased their risk. The average cost of a data breach in an SMB is ~$120,000 per incident.i 60% will go out of business within 6 months of an attack.ii 47% of LATAM SMBs surveyed had recently been the target or, or suspected they had been the target of, a cyberattack in the last 12 months. An additional 24% knew someone that was. COVID-19 pandemic has further exacerbated these concerns for SMBs as much of their workforce shifted to work-from-home, but they were unable to increase IT resources to secure connections. The result is, now they are even more at risk and, and looking to spend on cybersecurity solutions. In fact, 89% of LATAM SMBs identified cybersecurity as one of their top priorities and 58% said they would switch to a provider that offered comprehensive network-based security.

WOULD A CLEAR SECURITY SOLUTION MAKE YOU SWITCH PROVIDER?



This need created a clear opportunity for CSPs to provide network-bases security solutions especially tailored to meet the needs of SMBs at a very competitive price. The primary cybersecurity needs of this sector are:

- Protecting the corporate network from malware, phishing and other cyber attacks
- Preventing employees from accessing dangerous or inappropriate sites
- Protecting employees connecting from outside the corporate network
- Securing BYOD devices
- Extending protection to fixed and mobile devices when employees are connected outside the corporate network

Service Providers are in a unique position in the market because they are able to touch all network traffic in and out of increasingly complex SMB environments, on fixed, on mobile, and even on Wi-Fi, ensuring that workers' devices stay safe, whether at the office or at home. They can also leverage existing Customer Premise Equipment (CPE), taking advantage of existing relationships with SMBs, to expand into the security market and emerge as leaders for the low

end of this security market. They can leverage their preexisting relationship to upsell secure internet services as opposed to trying to push point products.

LATAM SMBs are willing to pay their service provider $5 USD per month network-based security solution

This opportunity translates into high penetration rates, increased ARPU and NPS, and brand loyalty for Service Providers in LATAM.

Allot research and industry experience has pointed to a growing market of SMBs turning to Service Providers for security solutions. Overall, 59% of SMBs reported that they are outsourcing their cybersecurity needs, much of that to service providers.[iii]

Summary

This survey reinforces that consumers and SMBs are very concerned about cyberthreats and are willing to do something about it. But most consumers are not IT security professionals, and most SMBS cannot afford an in-house IT security expert. Therefore selecting, implementing and maintaining reliable security tools for their home or business router and all their connected devices is therefore a challenging task. The many barriers to implementing a comprehensive solution leave most of your customers at risk. The good news is that **64% of customers in LATAM are willing to pay an additional monthly fee (average $5.00 USD) to take care of all their security needs from the network**.

At Allot, we help CSPs around the world increase ARPU and brand reputation by offering no-touch, network-based, security-as-a-service (SECaaS) solutions with parental controls.

LATAM service providers are at a critical crossroads where they must decide if they are going to add security-as-a-service to differentiate their brand, or whether they will let a competitor take the lead. This LATAM customer survey shows strong evidence that consumers, especially families with school-aged children, place a very high value on online safety and security and would gladly pay an additional monthly fee for a comprehensive, easy-to-manage solution and would even potentially change providers for such a service.

Key Takeaways

- LATAM mobile customers show high levels of awareness and concern about cybersecurity threats, yet a general uncertainly about exactly which steps they should be taking to protect themselves
- Consumers have implemented partial security solutions that cannot provide comprehensive protection against all threats, on all devices, no matter where or how they connect to the internet
- 82% are worried about their device getting hacked while connected to the mobile network

- 47% of consumers think the coronavirus has increased cyberthreats
- 95% said that their CSP should provide security solutions
- 63% of LATAM subscribers are willing to pay an additional $5.00 USD per month to their mobile provider to take care of all their security needs from the network
- 66% of parents are willing to pay their CSP an additional $4.50 USD or more for parental control features.
- **6 out of 10 of customers and SMBs said security was so important to them, they would switch to a provider with a clear security offering**

Solution: A Brief Overview of Allot Secure

Allot has a strong track record working with Service Providers providing solutions for both the consumer and SMB mass market. The *Allot Secure* offering has delivered Service Providers around the world very high penetration rates, increased revenue streams, increased ARPU, very high NPS and increased brand loyalty. The Allot Secure solution suite, with its varied product components, provides a proven path for Service Providers to protect their customers' mobile and fixed networks and even off-network connections.

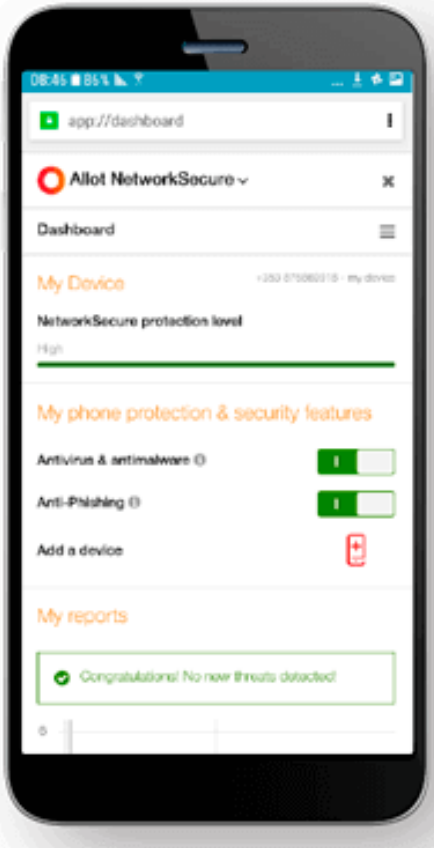
Allot Secure delivers network-based security to stop threats at the network level, far from customer smartphones, computers, and other connected devices. Because the protection runs in the network, no download is needed, it's compatible with any range of devices and operating systems, and it's always up to date to confront the latest threats, solving a huge problem for both mobile and fixed consumers and SMBs.

Allot Secure leverages the Service Provider network in the following ways:

Easy to deliver: A network-based cybersecurity solution makes it easy for operators to deliver protection directly to their customers, without the customers needing to install or update any applications. Network-based solutions must be multi-tenant and scalable to mass-market levels, dramatically revitalizing the VAS business model. Millions of end-users can be easily supported so even nominal monthly fees can generate millions of euros/dollars per month.

Easy to promote: The second advantage of a network-based solution is the ease with which it can be promoted, trialed, and converted into paid subscriptions – all through the network. CSPs can market the solution through a mix of text messages, banners, portal ads and site redirects. Once a customer agrees to a free trial of the solution, they can be instantly activated. The prospective customer is immediately protected and begins to enjoy the peace of mind that comes with network-based security. The CSP can easily push notifications and alerts that inform the end-user of all the harmful content and malware blocked by the solution, transparently and with no effort on the part of the customer. When it's time to propose converting to a paid subscription, the customer is well aware of the benefits and value that have been delivered effortlessly. This is the secret to Allot Secure consistent high adoption rates.

Easy to maintain: The third great advantage of this network-based solution is that updates and improvements are implemented once, by the CSP, and instantly go into effect for every user of the service. The users receive notification but need not take any action to enjoy the update. It's there, in the network, protecting them.



Allot Secure delivers the following security capabilities to subscribers:

Web Security with up-to-date threat intelligence and in-line anti-virus scanning to protect users from malware such as crypto-jacking, ransomware, and banking-trojans, as well as protecting devices from IoT-specific attacks such as Mirai and its variants. A good example is Anti-Phishing - to protect customers from falling victim to online scams that redirect to malicious websites that mimic legitimate ones in order to steal online credentials and/or infect user devices with malware. Unlike DNS solutions that cannot detect inner pages of legitimate sites with phishing attacks, Allot Secure blocks these too.

Another example is **Anti-Bot protection** to block bot "command and control" callback requests in-line, based on up-to-date threat intelligence, and to quarantine bot-infected endpoints. This is another advantage over DNS, for both infected IoT devices and endpoint devices since most bots avoid the use of DNS.

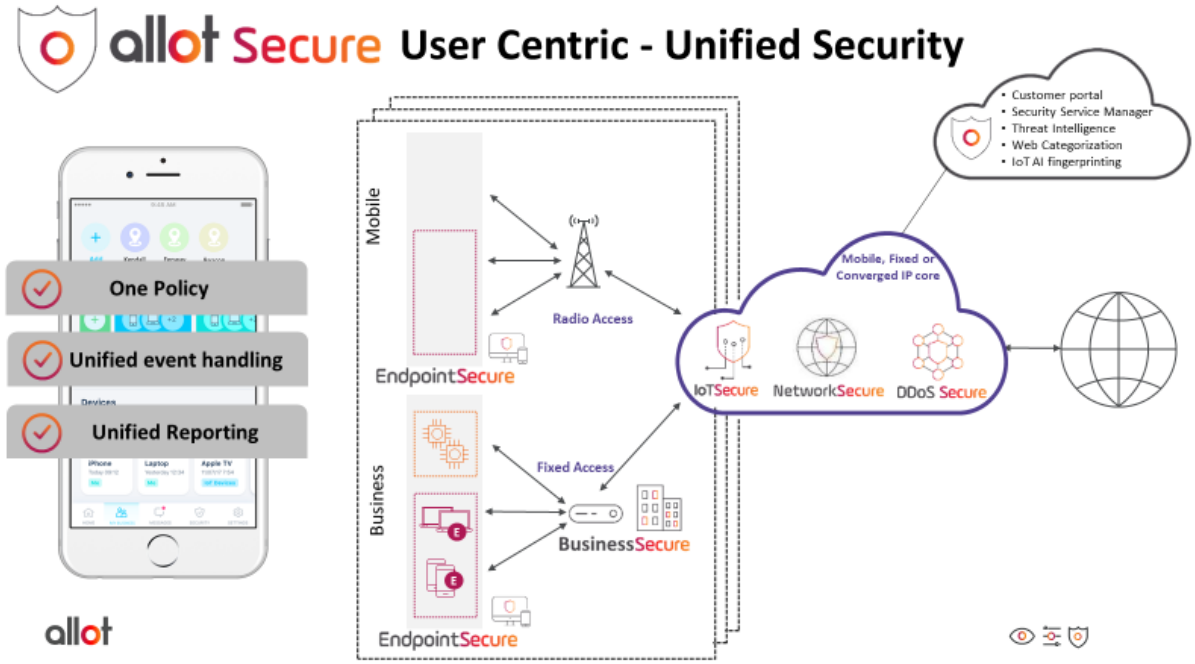
Content Filtering with a global database of web categories to allow consumers to exercise parental control and businesses to enforce acceptable-use policies. Content inspection is based on HTTP/S data and header inspection and does not rely on DNS, which can be bypassed by tunneling encrypted DNS requests to a 3rd party such as Google or Cloudflare.

Allot Secure is a platform that integrates security services for mobile, fixed and converged network subscribers, providing unified policy and reporting across multiple security domains. Allot Secure unifies network-based security with endpoint and CPE-

based security so CSPs can deliver branded security services to the mass market. The platform features a seamless customer experience for all three security layers and has been successfully deployed to 23 million end-users, reaching 50% penetration rates, increasing ARPU by 5% and dramatically enhancing customer satisfaction.

A 360° solution, the Allot Secure platform consists of the following components

- **NetworkSecure**: Secures mobile users and homes and applies parental/business policy control across all end users
- **BusinessSecure**: Secures smart, connected appliances and SMB offices by integrating security software with existing CPEs.
- **EndpointSecure**: An extension of NetworkSecure, for securing users off-network with a seamless customer experience.



The platform features unified management that simplifies configuration, settings, reporting and alerts, ensuring users are protected regardless of where or how they access the internet.

I. Kaspersky Lab Report, May 2018

II. 60% of Small Companies that Suffer a Cyberattack are out of Business within Six Months, Denver Post, March 24, 2017

III. Security in SMBs, Coleman Parkes Research for Allot, December 2019