allot
See. Control. Secure.

Position Paper

Switch to Security: Consumer Security Survey – North America 2020

October 2020

Table of Contents

Introduction

During May and August of 2020, Allot partnered with Coleman Parkes Research Group to survey 3,500 North American (Canada 1000, US 2500) mobile subscribers 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 similar surveys conducted in APAC, LATAM and Europe published by Allot in Q3 2020.

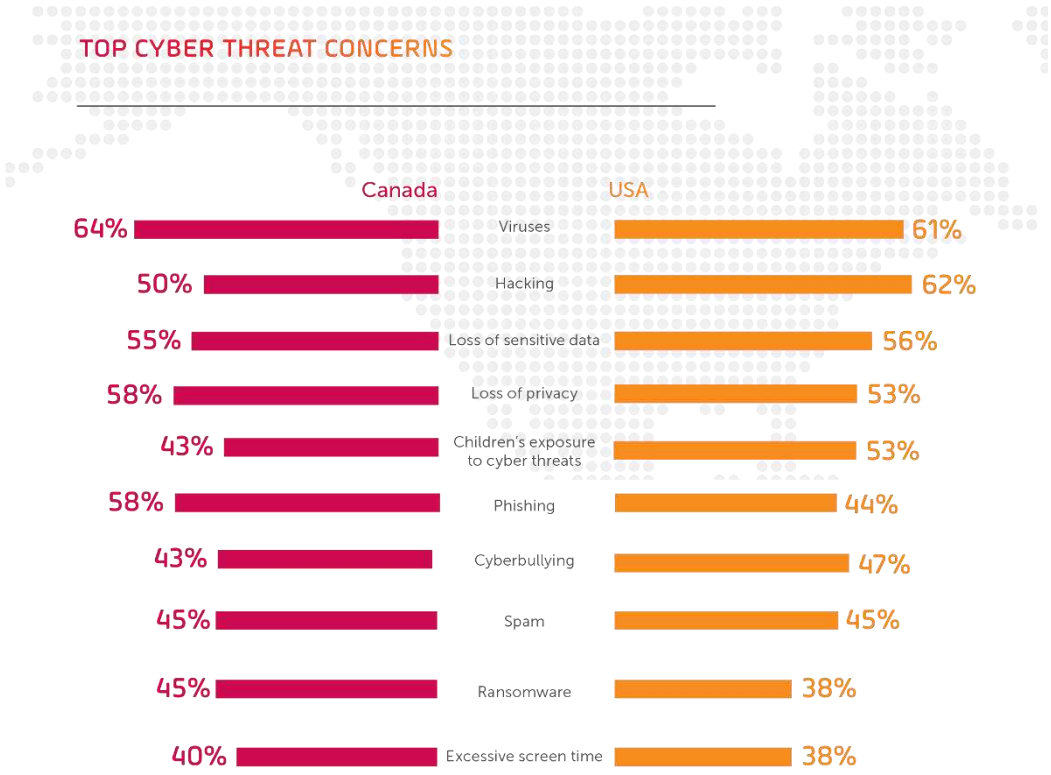
A large proportion believe that their CSP should provide protection against online threats and expressed a willingness to pay an additional monthly fee for an easy-to-use solution that protects all their connected devices at home and on the go. 70% of North American consumers surveyed said security was so important to them, they would 'definitely' or 'probably' switch to a provider with a clear security offering.

7 out of 10 consumers 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.

When asked which cyber threat they are most concerned about respondents cited viruses (US 61%, Canada 64%), hacking (US 62%, Canada 50%) and loss of sensitive data (US 56%, Canada 55%). In addition, parents with school-aged children are also highly concerned about protecting devices used by children from malware and viruses and excessive screen time.



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. Over half of North American respondents think there is added risk of security threats in the Coronavirus era, though Canadians are slightly less concerned (42%) than their US counterparts (54%).

1/2 of mobile consumers in North America 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. The majority of North American consumers have a security solution on their internet connected devices. Over two-thirds of Canadian respondents have a solution to control phishing, whilst over half of US respondents have a solution to control against a virus attack. Canadians are more likely to have solutions to protect against viruses (US 54%, Canada 62%), malware (US 48%, Canada 54%) and phishing (US 39%, Canada 69%). While Americans are more likely to have a social media monitoring solution installed (US 69%, Canada 39%). 10% of respondents in both countries reported not having any kind of security solution installed.

80% already pay an average $5.89 per month for some kind of partial security solution

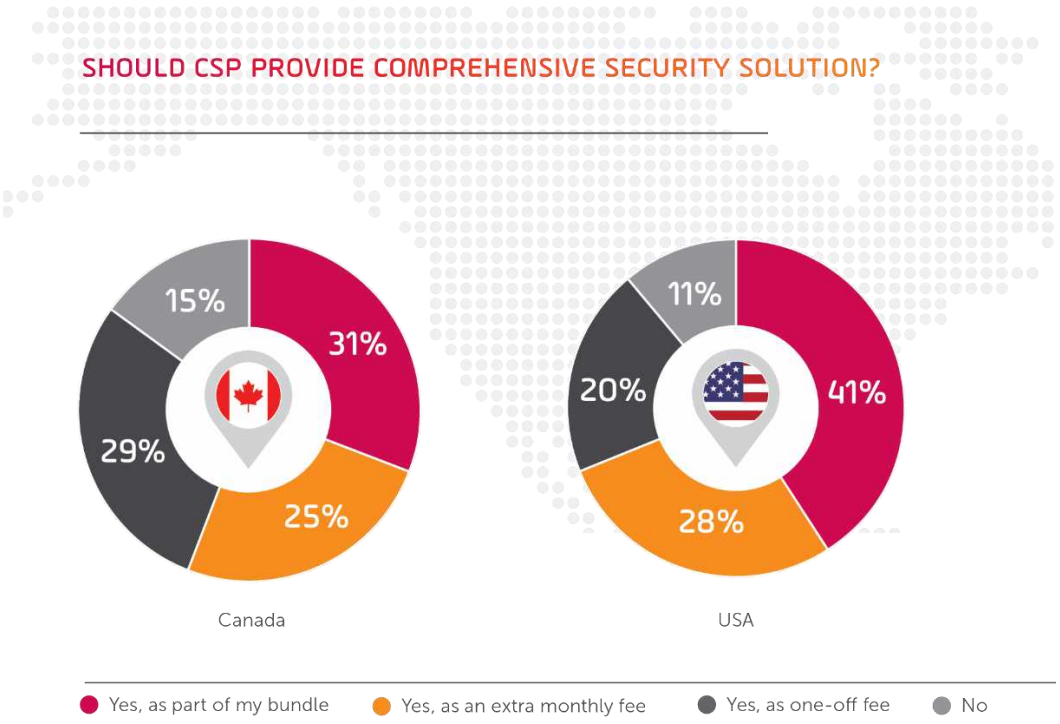
Many users installed free apps, but for those who purchased their security solution, they paid an average monthly fee of $5.60 (Canada) and $5.90 (USA). A fifth of Canadian consumers paid an upfront payment. On the one hand, this shows that the consumer market is motivated to acquire cybersecurity protection. 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. Roughly half of consumers 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

87% said that their CSP should provide security solution

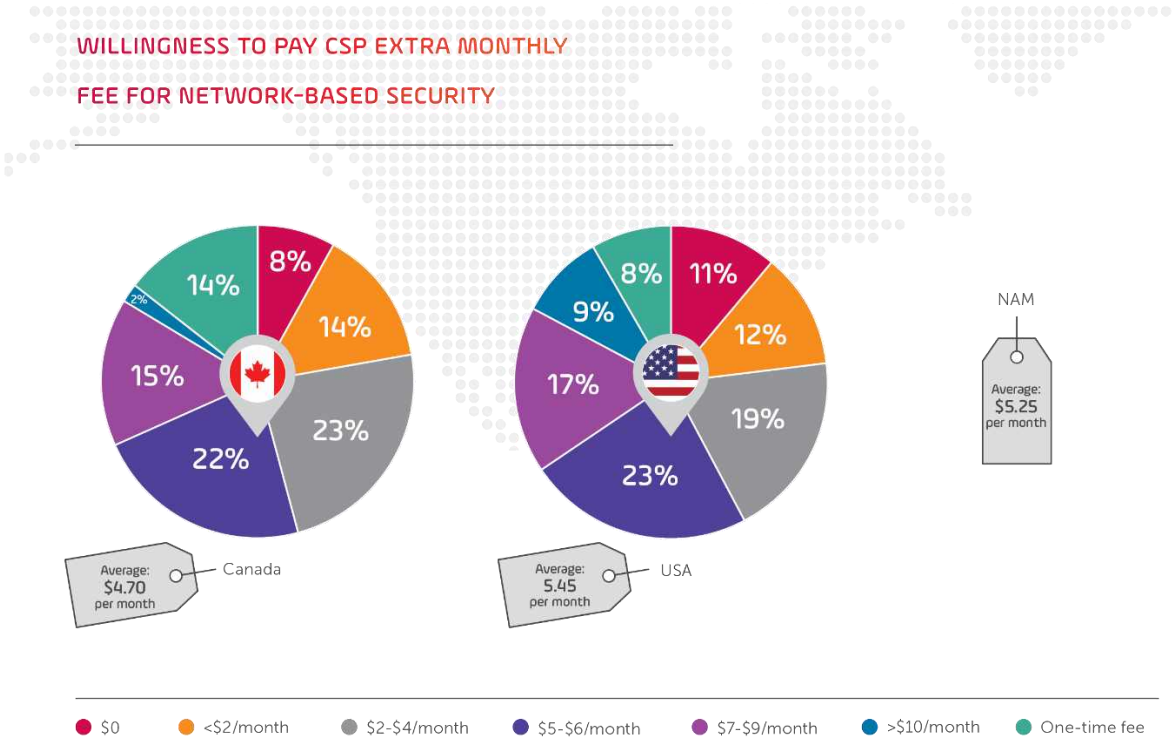
Perhaps most interestingly, though not surprisingly, 87% of respondents in this survey said that their service provider should provide security solutions. This is a strong vote of confidence that customers trust the provider to deliver quality protection. 41% of US and 31% of Canadian subscribers believe security should be provided as part of the bundle, 28% of US and 25% of Canadians said security should be provided by for an extra monthly fee 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.



Willingness to Pay

79% North American consumers are willing to pay their CSP an additional $5.25 per month for network-based security

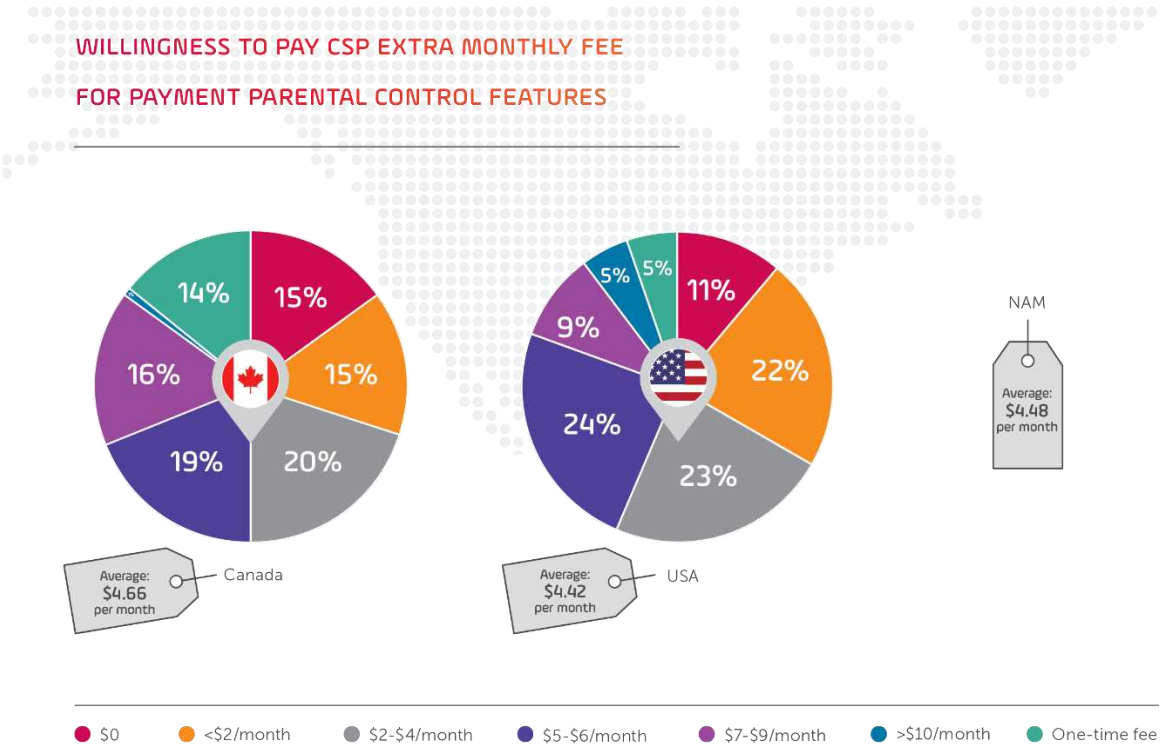
Taking it one step further, we asked mobile subscribers who had at least one security tool already installed, how much they would be willing to pay for a comprehensive, hassle-free security solution provided by their mobile carrier. The responses show a large percentage are willing to pay for such a solution. 79% of North American consumers are willing to pay their service provider an additional monthly fee of $5.25 for network-based security protection. Consumers in the US ($5.45) are willing to pay more on average than those in Canada ($4.70).



1.1.1 Parental Concerns & Controls

Naturally, parents across the US and Canada are highly concerned about their children's activity and safety online. Over half of North American parents stated that a parental control service is important to them – this figure is slightly higher (57%) amongst Canadian respondents, (53% USA). They very clearly articulated the type of parental control features they desire, notably, blocking inappropriate content (49%), social media monitoring and cyberbullying protection (47%), blocking inappropriate apps (43%), and location updates and alerts (41%).

North American consumers would be willing to pay **$4.48 on average per month** to be on a network with a better parental control feature. **60%** of North American parents are willing to pay their CSP an additional **$2-10 (average $4.48)** on top of their currently monthly fee for parental control features, while an additional 14% of Canadians indicated they would pay a one-time fee.



Summary

This survey reinforces that North American consumers are very concerned about cyberthreats and are willing to do something about it. But most consumers are not IT security professionals and therefore selecting, implementing and maintaining reliable security tools for their home and all their connected devices is a challenging task. The many barriers to implementing a comprehensive solution leave most of your customers at risk. The good news is that **79% of customers in North America are willing to pay an additional monthly fee (average $5.25) to take care of all their security needs from the network.**

60% of parents would be willing to pay an extra monthly fee for good parental controls. Together this is very strong evidence that marketing a network-based security solution that includes parental controls could be a very compelling offering to a large customer segment of families with school age children.

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.

Service providers in the US and Canada 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 North American 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 switch to another provider for such a service.

Key Takeaways

- North American 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
- 1/2 of North American mobile consumers think COVID-19 has increased cyberthreats
- 87% said that their CSP should provide security solutions
- **79% of North American subscribers are willing to pay an additional $5.25 per month to their CSP to take care of all their security needs from the network**
- 60% of parents are willing to pay their CSP an additional monthly fee for parental control features.
- **7 out of 10 of customers 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, offering 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 is compatible with any range of devices and operating systems, and is 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 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 is 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 consistently high adoption rates with Allot Secure.

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.

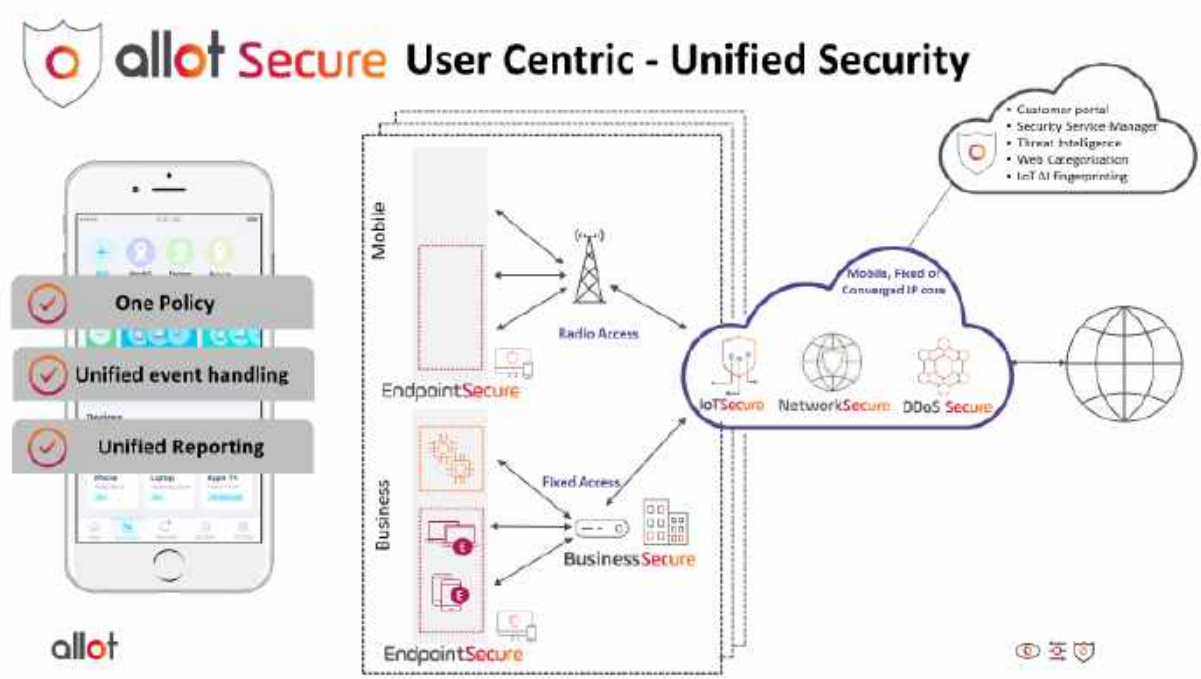
Content Filtering with a global database of web categories to allow consumers to exercise parental control and businesses to enforce acceptable-use policies. Content inspection is based on HTTP/S data and header inspection and does not rely on DNS, which can be bypassed by tunneling encrypted DNS requests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

For More Information

To learn more about Allot Network Security Solutions for Service Providers, download the Telco Security Trends Report:

How Effective are CSP Security Services for the Mass Market?

or watch this video: How Allot NetworkSecure Works.