allot
See. Control. Secure.

Cybersecurity Subscription Services for Consumers and Small Businesses

A Compelling Business Case for CSPs

April 2020

See. Control. Secure.

Contents

1 Introduction

Communication Service Providers (CSPs) traditionally have little success when offering security products and services to consumer and small business subscribers. Typically, they have offered endpoint security applications that gained very limited traction as mass-market solutions – with adoption rates of only 1 to 5%. These solutions suffer from inefficient onboarding processes, prices that are beyond private and small business customer budgets, and challenging updates that rarely occur. As we show in this document, there is an alternative solution that overcomes these obstacles.

With network-based Cybersecurity Subscription Services, CSPs can deliver their consumer and small business customers powerful, zero-touch protection against cyberattacks and unwanted content that overcomes the increasing complexities and vulnerabilities of today's communications landscape.

2 The Threat Landscape

Every day, across all markets, we see a growing number of mobile and fixed subscribers, both consumers and small businesses, who are increasingly vulnerable to cybercrime threats. Our research shows that a common threat come from phishing attacks designed to illegally collect personal information and access criteria. Other common threats include various types of malware, data theft, and cryptojacking, to name a few.

Most cybercrime is driven by money. From distributing malware and stealing users' credentials, financial gain is the biggest motive behind cyberattacks. Financially motivated actors have become more professional and have widened their range of techniques in order to make a profit. For example, phishing profitability is estimated to be hundreds of times more profitable than legal business endeavors.

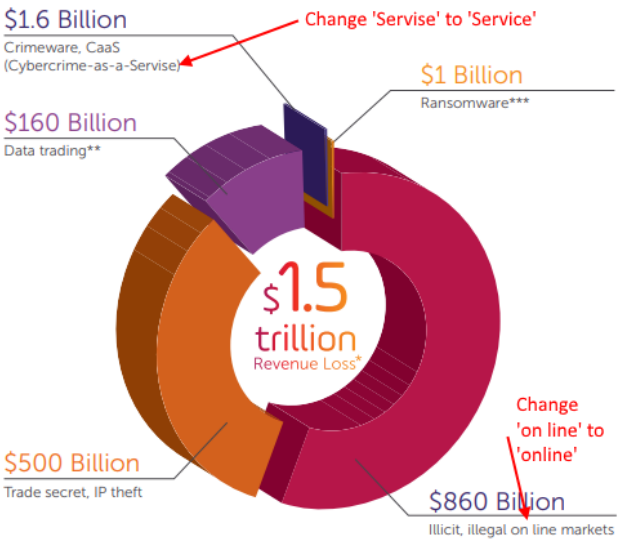
The International Monetary Fund ranks cybercrime third in dollar value as a global scourge[1] - while only a small percentage of real cybercrime is usually reported. Across the world, more than 1.2 billion adults have been the victims of cybercrime, with 867 million in 2018 alone (2018 Norton LifeLock Cyber Safety Insights Report). Of those who did experience cybercrime in 2018, 38% had a financial loss and spent 6 hours on

[1] https://www.imf.org/external/pubs/ft/sdn/2016/sdn1605.pdf

average resolving the crime. Beyond cybercrime, 117 million adults around the globe were impacted by identity theft.

The issue of cybercrime will become even more acute with the rollout of 5G across the world. 5G networks will have a higher security vulnerability due to a combination of several factors. First, it is anticipated that the number of IoT devices in 5G networks will be orders of magnitude higher; second, bandwidth per device will be much higher; and third, 5G networks' distributed architecture increases the number of vulnerable connectivity interfaces. These vulnerabilities pose a huge challenge to consumers and small businesses. CSPs would be well advised to find new ways to protect their customers.

As concluded within the recently published Allot Telco Security Trends report, *How Effective are CSP Security Services for the Mass Market?*, cybercrime is thriving and will continue to innovate and take advantage of the growing cyberattack surface due to the financial opportunities it provides. To protect their devices and data from increasingly sophisticated, automated and dynamic cyberattacks, consumers and small businesses require a level of security expertise that, for the most part, they just don't have. This expertise can, therefore, be provided by the CSP as a lucrative service to protect consumers and small businesses against the rising tide of cyberthreats.



* Totals are approximate

** Revenues derived from trading in stolen data, such as: credit and debit card information, banking log-in details, loyalty schemes, etc.

*** Revenues derived from extortions based on encrypting data and demanding payments

3 The Business Landscape

Meanwhile, CSPs throughout the world are, in general, experiencing declining ARPU, persistent customer churn, commoditization of what were once differentiating services, and cannibalization of network resources and profitability by OTT apps and services.

On top of all that, value-added services (VAS) have generally failed to gain traction, mostly due to cost, inconvenience and the prevalence of 3rd party apps that seemingly meet every need, dashing hopes for increased revenues. The attempts to counter these trends by marketing otherwise successful, large-scale business services and security solutions to consumers and SMBs has also been unsuccessful; These platforms do not scale down properly for small business and consumer use and, therefore, do not present a profitable option for CSPs.

Despite these obstacles, Allot has found a solution that works: Network-based Cybersecurity Subscription Services for Consumers and Small Businesses.

4 The Business Opportunity

Consumers are concerned about all kinds of cyberthreats and they're especially concerned about the perils of online shopping, and the threats presented by online banking and other online financial transactions.

A recent report from the European Commission shows that people are growing less confident about their capacity to stay safe online. Compared to 2017, significantly fewer Internet users think they can protect themselves sufficiently against cybercrime.

Through our own research, we see that more than 50% of mobile subscribers earnestly care about security and privacy and 45% are willing to pay for security as an additional service.

Furthermore, our own industry experience shows high market penetration among business customers, with more than 70% of SMB customers opting-in to paid services after an initial free trial period.

It's clear that consumers, as well as small and medium sized business customers, are willing to buy security solutions from communication service providers.

For CSPs, this represents a huge market opportunity – to step up and be "the hero" who protects people with a service that delivers security and peace of mind. Telecom

operators are in the ideal position to deliver this peace of mind as they are already the incumbent connectivity provider, delivering the broadband connection between mass market users and the online world. Because they own the data pipes, they can easily upsell security to deliver secure broadband instead of just connectivity.

In his January 2020 report about *The Future of Telecom*, Shally Tshuva of Deloitte indicated that security and privacy / cybersecurity are at the heart of business issues for telecom operators. "The threat from malicious use of networked devices is increasing along with ever-increasing connectivity." Along with that, he calls attention to the trend of, "carriers becoming centers of cyber expertise."

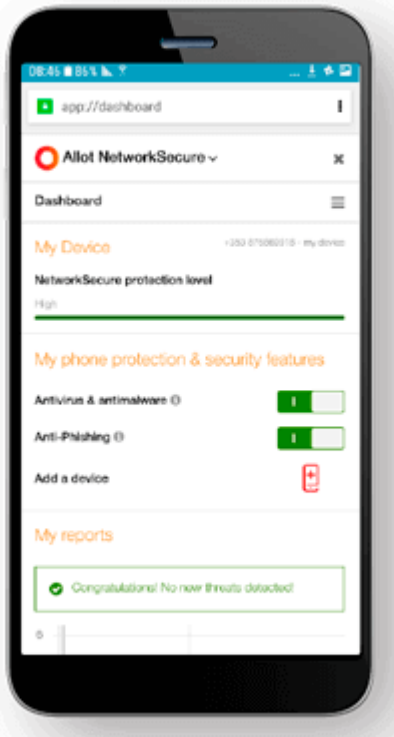
5 The Solution – A Brief Overview of Allot Secure

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 CSP 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 supported so even nominal monthly fees can generate millions of euros/dollars per month.

Easy to promote: The second, great 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 trial the solution, they can be instantly activated.. The prospective customer is immediately protected and begins to enjoy the secure peace of mind. The CSP can easily push notifications and alerts that inform the end-user of all the times harmful content and malware were 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 the high adoption rates we see consistently.



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 their subscribers:

Web Security with up-to-date threat intelligence and in-line anti-virus scanning to protect users from malware such as cryptojacking, 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.

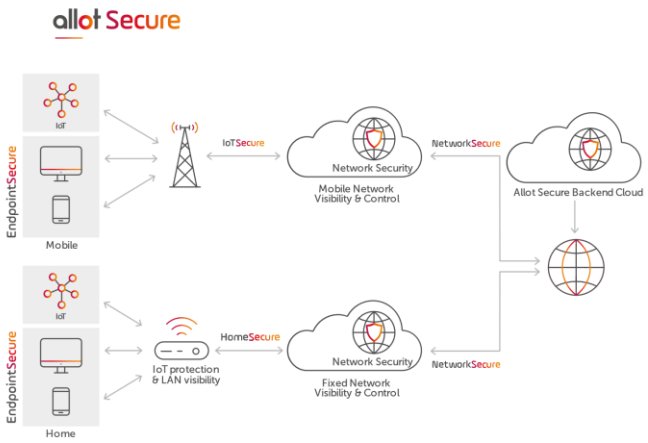
Allot Secure is a platform that integrates security services for mobile, fixed and converged network subscribers, providing unified policy and reporting across multiple security domains. Allot Secure unifies network-based security with endpoint and CPE-based security so CSPs can deliver branded security services to the mass market. The

platform features a seamless customer experience for all three security layers and has been successfully deployed to some 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

- HomeSecure: Secures smart, connected home appliances, and SMB offices by integrating security software with existing CPEs.
- EndpointSecure: An extension of NetworkSecure, for securing CSP customers off-net with a seamless customer experience.



The platform features unified management that simplifies configuration, settings, reporting and alerts, ensuring, for example, that kids are protected regardless of where or how they access the Internet. Once you set Internet category restrictions, for example by banning violent web sites, your child is prevented from accessing these sites via the CSP mobile network, while connected to your home network and even when accessing public Wi-Fi.

6 Case Studies

To combat the variety of threats out there, top mobile operators, like Vodafone, Telefonica, and Hutchison Drei, have turned to Allot Secure to protect their customers. They were not satisfied with the low adoption rate of endpoint solutions and the limitations of DNS security. The success of these projects is rapidly turning them into trusted security vendors, increasing ARPU and customer satisfaction.

Case Study: Huchison Drei Austria – Internetschutz

In August 2019, Hutchison Drei Austria launched "Internetschutz," a Cybersecurity Service solution powered by the NetworkSecure platform from Allot.

Drei offers "Internetschutz" as an add-on service to postpaid smartphone and data customers, who get a 30-day free trial that converts to an ongoing plan costing €1.5/month.

According to Martin Westhoff, Team Leader Strategy & Marketing Home at Drei, "More than a third of new customers who sign contracts in our stores choose to sign up for the Internetschutz service, and the month-over-month adoption rate in the first 4 months averaged 75%. This is a very encouraging trend that indicates the success of the Allot cybersecurity solution and related services."

Case Study: Telefonica Empresas – Conexión Segura Empresas

In Spain, Conexión Segura Empresas, the cybersecurity solution developed for SMBs by Telefónica Empresas and Allot, prevents threats derived from browsing the internet in the SMB environment and extends protection to fixed, fiber-connected devices, as well as mobile devices.

Within the first two months, the Spanish SMBs subscribed to Conexión Segura Empresas avoided more than 80,000 potential cybersecurity incidents. Of those, more than 89% of blocks occurred when users tried to access risky domains or websites, as a result of 'phishing'.

Since launching, the Conexión Segura Empresas service has gained thousands of subscribers and is experiencing, on average, more than 100 new and existing SMB customers subscribing per day.

7 Conclusions - A Perfect Storm

The combination of an expanding threat landscape, growing security awareness among consumers, and the ability of CSPs to deliver effortless, unified security through the network has created a 'perfect storm' opportunity for CSPs. They can drive new revenue, increase customer satisfaction, and differentiate their brand by selling not just connectivity, but truly secure broadband. Network-based cybersecurity services for consumers and small businesses are already generating hundreds of millions of dollars in new revenue for CSPs and the market has only just begun to take off.

Now, more than ever before, service providers are in a unique position to protect their mobile subscribers by offering network-based cybersecurity as a mass market cybersecurity solution. By providing this valuable service to the market at a cost as low as a couple of Dollars/Euros each month, or even less, CSPs can generate significant revenue while protecting customers and strengthening loyalty to the brand.

Although this is an emerging market, the initial results are in and the business case for network-based security is compelling. The numbers clearly indicate that we are experiencing a "sea change." An increasing number of mobile network operators are adopting this strategy, riding the wave and taking advantage of the growing trend of Cybersecurity Subscription Services, which are providing convenient, comprehensive protection to customers, and a growing source of revenue for CSPs.

www.allot.com **sales@allot.com**

Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA - Tel: +1 781-939-9300; Fax: +1 781-939-9393; Toll free: +1 877-255-6826
Europe: NCI–Les Centres d'Affaires Village d'Entreprises, 'Green Side' 400 Avenue Roumanille, BP309 06906 Sophia Antipolis, Cedex France - Tel: +33 (0) 4-93-001160; Fax: +33 (0) 4-93-001165
Asia Pacific: 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104, Tel: +65 6749-0213; Fax: +65 6848-1015
Japan: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 - Tel: +81 (3) 5297 7668; Fax: +81 (3) 5297 7669
Middle East & Africa: 22 Hanagar Street, Industrial Zone B, Hod Hasharon, 4501317 Israel - Tel: 972 (9) 761-9200; Fax: 972 (9) 744-3626