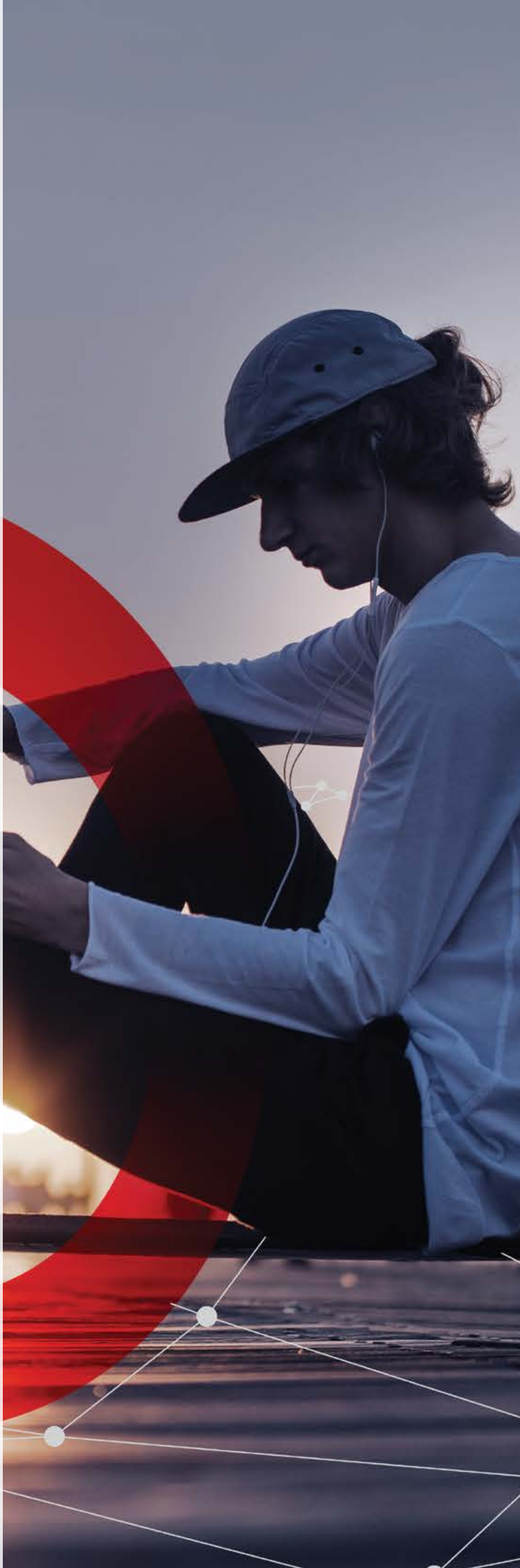
allot
See. Control. Secure.

Allot Mobile Security Trends - Q1 2018

BUILDING REVENUES, DIFFERENTIATION AND BRAND LOYALTY WITH SECURITY AS A SERVICE



EXECUTIVE SUMMARY

AS THE DIGITAL WORLD BECOMES MORE PREVALENT, MOST CONSUMERS ARE UNEQUIPPED TO DEAL WITH THE CONTINUOUSLY CHANGING THREAT LANDSCAPE THAT ACCOMPANIES IT.

The massive growth in mobile apps, content and traffic is accompanied by an increased cyber risk from an ever-evolving set of broad and sophisticated criminal activities. The result is broad concern and considerable damage to the individuals affected. The 2017 Identity Fraud Study, released by Javelin Strategy & Research, found that $16 billion was stolen from 15.4 million U.S. consumers in 2016, with mobile phishing being a significant source.

The average consumer is unaware of most of the potential threats and is unable to deal with them. On the other hand operators are in a prime position to help subscribers avoid dealing with these complexities and mitigate the risks. With their considerable in-house cyber security expertise, their existing relationship with consumers and the right tools, operators can mitigate risks and conceal complexities without any effort or action required on the part of the consumer.

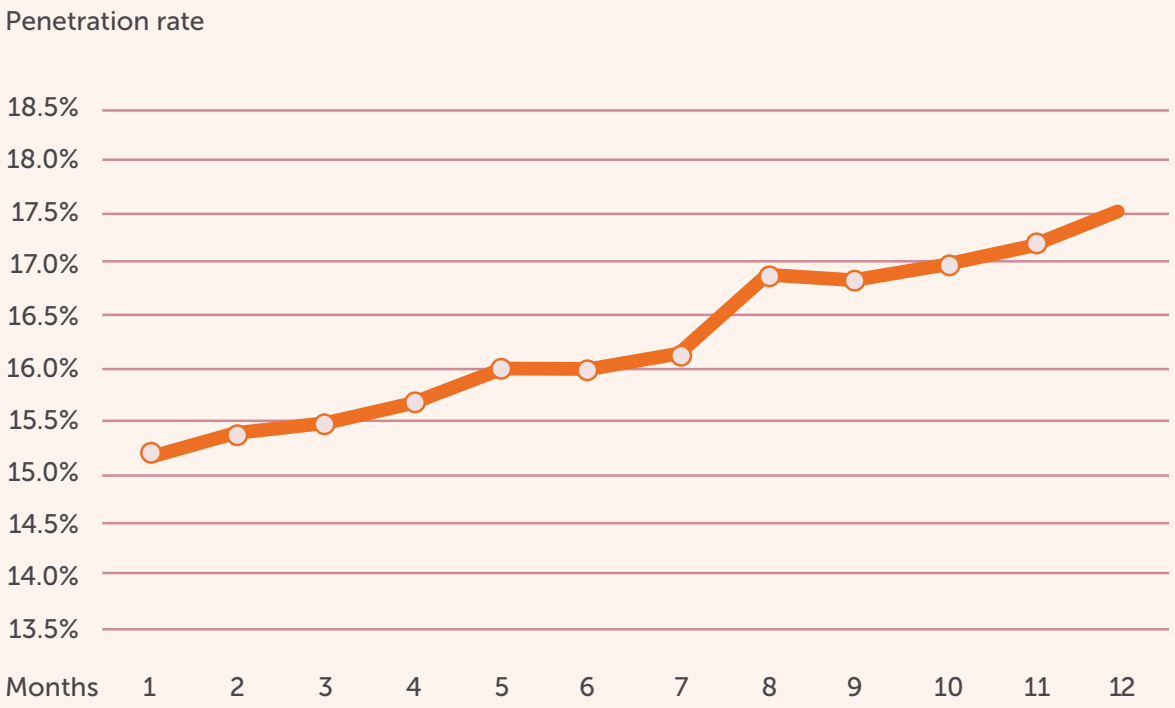
As consumer awareness grows with every publicized attack, demand for security services is growing and is has become key for operators wanting to differentiate their brand, re-engage with customers and put the brakes on further ARPU erosion. Historically operators have spent millions marketing legacy device-based security apps, which have consistently underachieved, with typical penetration rates of 3-5%.

On the other hand, network delivered security services have proven to be significantly better for both operators and their customers, with "Try and Buy" opt-in services achieving penetration rates of 12% to 15% while "Promotional" opt-out services performing even better with penetration rates of 40% to 60%. In addition to that, customers subscribed to security services demonstrate much higher levels of satisfaction with a 2-3 fold increase in customer Net Promoter Score (NPS) when compared to regular customers.

Mobile operators rolling out Security as a Service (SECaaS) have finally found the right model to build a sustainable competitive advantage.

EXECUTIVE SUMMARY

COMBINED OPT-IN & OPT-OUT SECURITY SERVICE PENETRATION RATE ACROSS 8 OPERATORS[1]



→ [1] First 12 months of operation after a 2-6 month trial or limited availability period

OPPORTUNITY KNOCKS

The motivation for CSPs to provide security service to customers is three-fold

1 TRUST AND LOYALTY

According to our last Allot MobileTrends Report , mobile customers are looking for a trusted partner with the right level of expertise to handle the security challenge for them. Providing such a service enables CSPs to build on their trusted relationship and protect their customers from significant risk.

The opportunity comes in the form of increased engagement with customers and the possibility of building a greater perceived value in terms of each customer. This results in increased customer loyalty, higher customer satisfaction (measured typically through Net Promoter Score, NPS) and lower churn rates.

As more and more devices are connected to the Internet and ever more data is exchanged, there is a need to create a more secure digital environment where people can safely work, socialize and shop. We want everyone to enjoy the benefits of connectivity without having to worry about being hacked or have their privacy violated.

KPN annual report 2016 – pg.40

OPPORTUNITY KNOCKS

The motivation for CSPs to provide security service to customers is three-fold

2 BRAND DIFFERENTIATION

Most CSPs now recognize that differentiation is a key strategy to avoid the "race-to-the-bottom" and break out of the commoditization trap that many markets have fallen into. To stand out from the crowd, each CSP must identify, build-out and evangelize new services that can deliver a clear and positive experience that will change the brand perception.

Building and maintaining a positive, high profile brand reputation is vital for CSPs, and that means delivering on their brand promise in every customer interaction and experience. Putting security front and center proclaims the CSP is alert and responsive to vulnerabilities and threats, but also clearly states the company is a secure brand that customers can trust.

For our customers, data privacy and security are very important and hence are a vital differentiator in competition. We guarantee our customers that we will handle their data securely and confidentially. We also see data privacy and security as a growing business area, which we want to significantly expand with existing and new security solutions.

DT annual report 2016

→ [2] https://www.allot.com/mobiletrends-q1-2017-v1/

OPPORTUNITY KNOCKS

The motivation for CSPs to provide security service to customers is three-fold

3 REVENUE GENERATION

Since the launch of the iPhone back in 2007, CSPs have been struggling to offset the decline in their legacy voice and messaging revenues. Launch of high-speed data connectivity services and "triple pay" bundles (voice, data and TV) has been a key focus in the last decade, but at the expense of huge investments. Any new value-added service that can clearly demonstrate new, profitable revenue stream would be a welcome addition.

The 2020 security ambition is to have security at the core of everything the company does, in order to protect people in their digital life. We aim to continue growing revenues and significantly improving our efficiency..

The key to our future success lies within the(se) opportunities.

Telenor annual report 2016

OPERATORS ARE BEST POSITIONED TO DEAL WITH THE CYBER EPIDEMIC

EXISTING RELATIONSHIP

Operators have an ongoing rapport with customers and are actively engaged with them across all relevant touch points, including online and offline channels.

BUILT-IN EXPERTISE

Mobile operators have dedicated security teams with the ability to integrate security systems in the network that are always up-to-date and provide the best solution to combat existing and future threats.

REMOVE COMPLEXITY AND MINIMIZE RISK WITHOUT CUSTOMER ACTION

The clear majority of customers are ill-equipped to deal with the increasingly complex cybersecurity threat landscape and yet, in spite of growing awareness, the minimal level of effort required to activate a security service often results in inaction.

Operators are in a position to deliver personalized, zero friction security services from the network that result in high levels of adoption.

Allot MobileTrends Report H1/2017 found that 61% of global respondents said they would like to buy a security service from their CSP for their connected devices

→ [3] https://www.allot.com/mobiletrends-q1-2017-v1/

COMING FULL CIRCLE WITH A BETTER UNDERSTANDING

Many operators have looked at providing security services to customers in the past, without much success. In most cases the solutions were based on a revenue share model with an anti-virus applications developer. Operators would rebrand a standard app, promote the service and implore subscribers to download, activate and pay for the application

The lack of success for the app-based model stems from several factors:

- **Service activation friction**
  - Non-operator device owners must be motivated to download, install and then buy an app/subscription - this has proven to be a very difficult task. The typical penetration rate that CSPs have achieved in the past pushing for 3rd party security apps has been no more than 3-5%.

  - Operators have tried to overcome the download and install issue by preloading security apps into operator-provided devices. Many mobile customers see this intrusion as bloatware. In addition, and more importantly, there is still considerable friction in motivating customers to activate and pay for pre-installed apps and to overcome the perception that a security app will impair phone performance and battery life.

- The application vendors themselves typically have a very limited insight into how the mobile operator business works and even less knowledge of operator networks and infrastructure.

- Marketing an app is significantly different from marketing a service. The core business of an operator is to sell services based either directly on their network or derived from the networking expertise that they have developed. App sales are often one-off and typically not aligned with an operator's core competence.

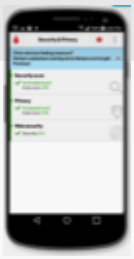
- Operators tend to carry the bulk of the risk in this model. App vendors may be required to customize the GUI, but the operators must spend big on marketing to achieve a modicum of success.

→ [3] https://www.allot.com/mobiletrends-q1-2017-v1/

→ [4] The term bloatware refers to "Applications — usually unwanted — that are preloaded onto a device." as defined by the Android Dictionary - https://www.androidcentral.com/dictionary

COMING FULL CIRCLE WITH A BETTER UNDERSTANDING

verizon VERIZON SECURITY & PRIVACY APP



Powered by McAfee Active Protection

Security & Privacy is a security app for your mobile device that helps protect it from malicious apps, spyware and other potential threats to your privacy. It's already installed on Verizon Android® devices and is included with your service for no additional charge.

VIEW HERE

Reliance jio JIOSECURITY APP

Powered by Norton Mobile Insights

It identifies dangerous websites and scans downloaded apps, app updates, and SD memory cards to detect and eliminate threats that are designed to steal your information for money. More importantly, Jio Security provides proactive virus protection against risky apps.

VIEW HERE

telenor TELIA SAFE

Powered by F-Secure

Telia SAFE that has been developed in cooperation with F-Secure is more than just an antivirus – it protects both your computer and all your smart mobile devices.

VIEW HERE

Many operators attempt to resell mobile security apps. The bottom line is that the effort and costs required to motivate customers to install, activate and pay for an app-based service is often cost prohibitive. There is a better alternative!

WHAT MAKES SECURITY AS A SERVICE (SECaaS) RADICALLY DIFFERENT

Security as a Service (SECaaS) is defined as a business model in which service providers integrate their security services into [their infrastructure and deliver it] on a subscription basis, providing it more cost effectively than most individuals or corporations can provide on their own, when total cost of ownership is considered.

The SECaaS approach provides significantly greater value than the app-based approach, both for the customer and the operator. SECaaS is by definition a network-based service that enables the operator to take full advantage of the fact that it owns the network. The SECaaS approach means the service is tightly integrated into the operator's network infrastructure, system and more importantly into their business strategy. SECaaS significantly reduces onboarding friction, bypassing the number one barrier to successful implementation of security services. Customers are significantly happier (as customer satisfaction metrics show), and express an increased "peace of mind" regarding security since it is the operator who is responsible for updating and maintaining the security infrastructure.

	SECaaS	Device-based Security Apps
Go-to-market -strategy	Inherently suited to try/buy or opt-in/out campaigns as it can be switched on by operator – no customer activation required	Too much friction, need to install, activate and pay.
Recurring revenues	Yes	Limited, and the majority goes to the app developer
Onboarding Campaigns	Mass informed on-boarding and activation accelerates penetration	Activation is at the discretion of the individual customer
High penetration	40-60%	3-5%
Customer satisfaction (NPS impact)	Very High – customers are protected without having to take any action. This increases loyalty and reduces churn.	Significant probability of negative impact due to app installation and support issues

[5] Wikipedia - https://en.wikipedia.org/wiki/Software_as_a_service

[6] NPS – Net Promoter Score https://en.wikipedia.org/wiki/Net_Promoter

THE (NEW) BLUEPRINT FOR SUCCESSFULLY ROLLING OUT SECURITY AS A SERVICE

The task of defining, building and launching new value-added services (VAS) in mobile operators is often assigned to the product strategy or marketing teams. While they may lead the process, they cannot achieve success alone. Successfully taking a service from idea to launch is a complex process that requires cross-functional collaboration, involving professionals from several departments and external expertise is often required.

Launching new VAS services in mobile operators tends to follow a tried and tested process. Below is an outline of the stages with regards to launching SECaaS.

Stages	Device-based Anti-X Apps
1 **Determine business case, define strategy and success**	Determine the business case with a clear definition of success in terms that are aligned with the company's objectives
2 **The Engagement Model**	Decide the appropriate go-to-market model or combination of approaches based on customer segmentation. This may be influenced by region, demographics and regulation
3 **Deployment and Integration**	Collaboration between departments to successfully deploy and integrate SECaaS into the network and IT systems
4 **Service launch**	Sales, support and other teams will need to be trained. Marketing plans will need to be in place, focused on achieving the clearly defined goals.
5 **Post launch**	Following the launch, marketing and sales will need to be focused on increasing penetration and keeping customers engaged

→ [6] NPS – Net Promoter Score https://en.wikipedia.org/wiki/Net_Promoter

DEFINE STRATEGY, SUCCESS AND GOALS

STAGE 1

The first step in the process is to define a clear marketing strategy. The product strategy manager will begin by researching, speaking to vendors, documenting alternatives and talking to commercial and technical departments. At this point this interest is not just about security capabilities, but capabilities around awareness and engagement are critical, as is finding a partner that understands how to deploy and market security as a “service” and has demonstrated success working with operator marketing teams to bring the service to market.

THE BUSINESS CASE

The product strategy manager must bring a compelling business case, including benefits, impact statement and a detailed cost vs. revenue analysis to justify the undertaking. Detailed discussions with other departments such as network operations and planning,

IT and even legal teams will be key in determining if the project is feasible and possible deployment strategies and costs and later creating buy-in from the various departmen.

Strategic focus area	{determined by corporate focus areas)	**Contributing KPIs**	Penetration rate; NPS; Brand impact; churn rates; revenue
Objectives	Add new service based on market need in order to attract more customers to a "secure network", increase stickiness/engagement with customers and generate new revenue streams.		
Operator BUs & others	Departments and 3rd party — vendors, integrators	**Estimated Budget**	Deployment, integration, marketing, training ,etc
Project Context	• Moving towards new technology and consumer services • Developing new methods for revenue generation • Respond to customer and market needs		
Project Benefits	• Brand differentiation as "most secure operator" or "your privacy is our business" • Grossing customer satisfaction, stickiness and lowering churn • Increasing revenue and profit		
Cost Analysis	• Cost of products/solution • Cost of deployments and support, sites, config changes, power, etc...		

→ [1] Sample of internal SECaaS Business case template

THE ENGAGEMENT MODEL

Once the project has received initial approval, the next step is to determine the best engagement model. The engagement model should be selected in accordance with the defined goals for the local market and the local/regional regulatory framework.

For example, if brand positioning is the only concern, the service may be offered for free to all subscribers, or just to premium subscribers. The engagement model selected will have a significant impact on the penetration rates of the service. For paid services, there are two primary alternatives, "Try and Buy" and the "Promotional" model.

ENGAGEMENT MODEL 1: TRY-AND-BUY

With the Try and Buy model, the service can be simply switched on for a given set of subscribers (for example: a customer segment for a given tariff) for a set period, typically 1-3 months. During that time, subscribers first should be told about the upgrade, and then they should be frequently reminded of the benefits and value of the service.

It is very important to emphasize that customer awareness is essential for the success of the service. This can be achieved via periodic messages and updates about evolving threats and how they personally have been protected.

Toward the end of the trial period, customers are prompted to opt-in to the monthly service.

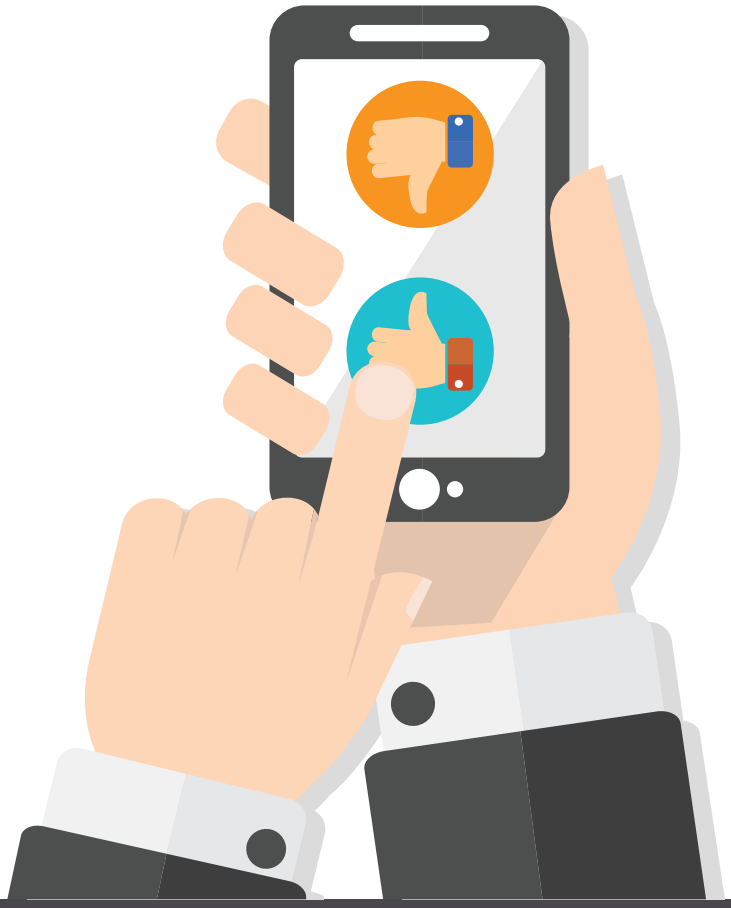
Existing results show that try and buy campaigns result in penetration rates of 12-15% when customer awareness is well taken care of. This is a huge improvement over the 3-5% penetration rates of the app-based approach.

ENGAGEMENT MODEL 2: PROMOTIONAL "OPT-OUT"

The Promotional "opt-out" model is a commercial bundle with an automatic promotion. This model sees the service switched on for all subscribers or subscribers in a predetermined segment, including new customers. The service is provided free of charge for a set period, typically 1-3 months. This model has a "bad reputation" in some countries, as it may have been abused in the past by CSPs for selling value added services.

However, in current SECaaS deployments it has proven to be a model that generates both high penetration and high customer satisfaction (a "dream product," win-win for all, except for cybercriminals). As in the Try and Buy model, subscribers need to be frequently reminded of the benefits and value of the service in terms of updates about evolving threats and how they personally have been protected. At the end of the period, subscribers are prompted to opt-out. Subscribers who decline to opt-out are then charged monthly for the service.

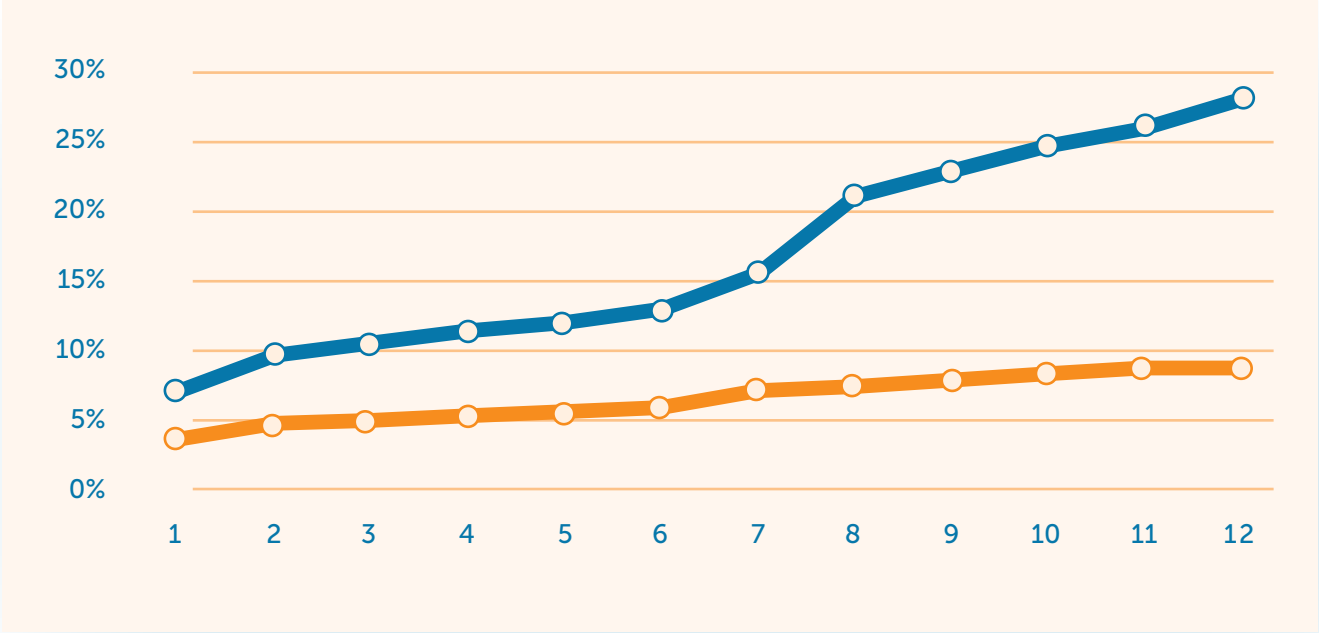
Operator numbers show Opt-out campaigns can result in penetration rates of 40-60%. This is a massive improvement on the 3-5% penetration rates of the device-based approach



COMPARISON: OPT-IN VS. OPT-OUT

Below is a graph showing the comparison in penetration rates over time for similar operators in similar markets by engagement model . Both these engagement models show tremendous improvement over the device/client based approach.

OPT-IN VS. OPT-OUT ACHIEVED PENETRATION RATES IN COMPARABLE MARKETS - FIRST 12 MONTHS



→ [7] First 12 months of operation after a 2-6 month trial or limited availability period

DEPLOYMENT AND INTEGRATION

STAGE 3

The relevant operator departments work closely with the selected vendor to deploy the service elements within the network and integrate it with the relevant IT services. Below is a checklist of the common steps

MARKETING THE SERVICE

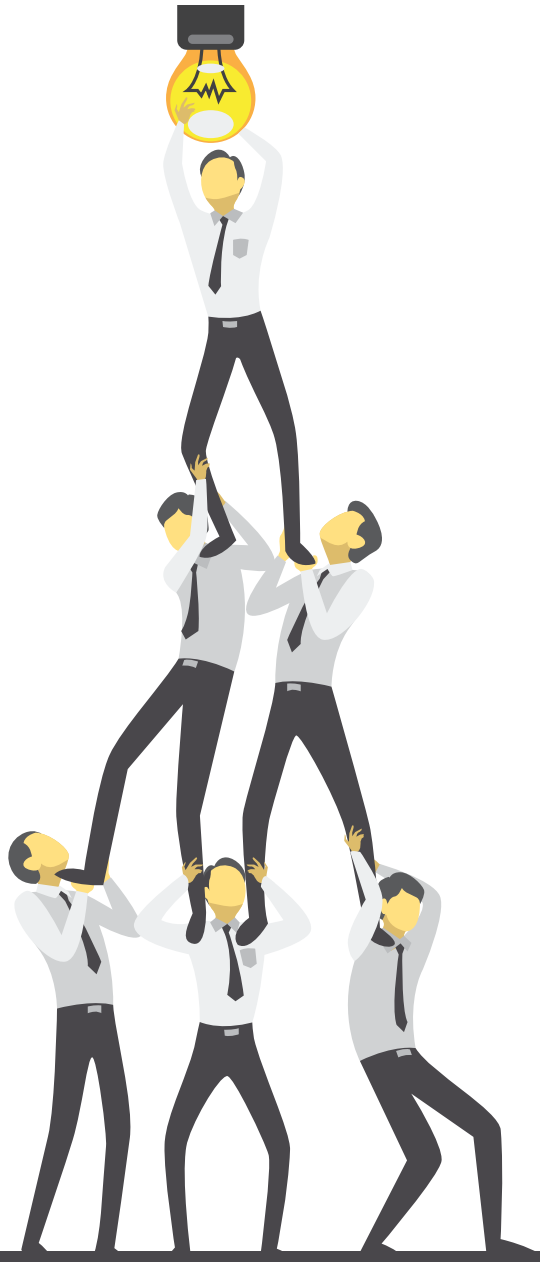
STAGE 4

Marketing teams have by now determined the engagement model, brand strategy and segmentation required for the service launch. At this point, the Marketing team develops tactical plans for an omni-channel marketing campaign that includes outreach and engagement through digital (online, social, and SMS) and physical channels (instore promotion/sales). The launch may be accompanied by a media blitz and promotional effort that may include radio, TV digital and billboard advertising.

During the initial deployment period, a network based system will provide reports on quantity and types of malware that customers are exposed to. These reports will enable the operator to describe the region-specific threat landscape and provide relevant security best practices that the operator can publicize in order to position itself as the "national authority" and information service on cyber threats, raising awareness and its own profile as a trusted source and advisor.

The Marketing strategy should be oriented to push for bundles with Tariffs: Opt-Out (if possible) and always "informed" or alternatively, to conduct a massive Try & Buy campaign. The customer-oriented message, utilizing massive consumer channels (ATL if possible, and online, social networks, etc.) regarding cyber threats and the benefits of the new services will be key to a successful launch. Rolling out the senior management will help build credibility around any new positioning that may have been developed.

The pre-launch stage is the time to training sales people on the benefits and key messages of the service. It is important to communicate product advantages clearly, for example, Automatic Activation from the Network, Multi-device Security (On-Net), Complementary with Off-Net App, Parental Control / Schedules, and the like.



MARKETING THE SERVICE – MEASURING SUCCESS

STAGE 4

Penetration is the most important key KPI for most operators. 10-15%% penetration in the first 6-12 months is considered a good but surmountable target, and from there growing to 40-60% (as it has been demonstrated in live deployments).

NPS figures provide a supplemental indication on how the new service is being received and the longer-term viability. In massive deployments, NPS numbers have seen an increase between 2 and 3 fold for customers with the service.

It can be concluded therefore that SECaas can have a dramatic impact on customer satisfaction, while generating revenues and brand differentiation

CUSTOMER SATISFACTION

Operator numbers show an improvement of 2 or 3-fold in **NPS** which is not uncommon as customer are highly engaged and feel more secure with the overall operator service.

KEY TAKEAWAYS

A network based approach to Security as a Service has proven to be remarkably successful. This success can be clearly measured in terms of service penetration rates, customer satisfaction, revenue generation and significant differentiation of the operator's brand.

The comprehensive blueprint presented in this report along with clearly defined and agreed upon goals, will enable operators to emulate the success of service providers who are already reaping the rewards of this innovative approach.

Deploying network based security transforms the network into a secure network for your customers. This is not a trivial distinction as it is aligned with your core business of delivering quality data services.

Allot Mobile Security Trends

Q1 2018

About Allot Communications

Allot Communications (NASDAQ, TASE: ALLT) is a leading provider of security and monetization solutions that enable service providers to protect and personalize the digital experience. Allot's flexible and highly scalable service delivery framework leverages the intelligence in data networks, enabling service providers to get closer to their customers, safeguard network assets and users, and accelerate time-to-revenue for value-added services. We employ innovative technology, proven know- how and a collaborative approach to provide the right solution for every network environment. Allot solutions are currently deployed at 5 of the top 10 global mobile operators and in thousands of CSP and enterprise networks worldwide.

www.allot.com | info@allot.com

Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA · Tel: (781) 939-9300 · Toll free: 877-255-6826 Fax: (781) 939-9393

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 67490213 Fax: +65 68481015

Japan: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 · Tel: 81 (3) 5297-7668 · Fax: 81(3) 5297-7669

Middle East and Africa: 22 Hanagar Street, Industrial Zone B, Hod-Hasharon, 4501317, Israel · Tel: 972 (9) 761-9200 · Fax: 972 (9) 744-3626

D265053 Rev.1