FROST & SULLIVAN

INDEPENDENT EQUITY RESEARCH

allot

Q2 and Update Initiation Report 24 Aug. 2020

Today's forms of communication have made the world into a very small place. We can easily communicate with our families, friends, and colleagues **via our cellular network,** to message them about the latest episode of our favorite show, streamed **via our home WiFi network**. Because these networks have become such a vital part of our lives they have become a vital asset for communication service providers (CSPs) that supply us with cellular, internet, and other services.

Allot Ltd. (NASDAQ, TASE: ALLT) is a B2B2C software company with over 20 years of experience that focuses on Network-based Security Solutions and Network Intelligence Solutions. These solutions enable entities such as communication service providers and enterprises to secure and optimize the digital experience of their users. Allot's motto is "See. Control. Secure." and it is a precise definition of the company's value proposition. The company allows its customers to see what is going on in their network, control their network to give the best experience to end users on all connected devices, and secure all of these devices against threats. It does this while providing network insights that save its customers significant capital and while creating new revenue streams for them. In essence, Allot empowers its customers to get more out of their networks.

The Company's solutions are deployed globally for network analytics, traffic control and shaping, and network-based security including mobile security, DDoS protection, IoT security, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed, and cloud service providers and over 1000 enterprises. Their network-based security as a service solution has achieved over 50% penetration with some service providers and is already used by over 23 million subscribers in Europe.

23% increase in Q2 revenue YoY; 2 new recurring revenue deals signed since May Q1 earning call; Allot consistently hits our progress targets, target price increased to 46.85 NIS / 13.6 USD

Stock Exchange: NASDAQ / TASE

Ticker: ALLT

Sector: Technology

Sub Sector: Software/Internet

Stock target price:

46.85 NIS / 13.6USD

Closing price: NIS 37.24
Market cap: 1.31B NIS
# of shares: 35.1 million
Stock performance (YTD): 20%

Lead Analyst
Dr. Tiran Rothman

Frost & Sullivan Research & Consulting Ltd.

T: +972 (0) 9 950 2888
E: equity.research@frost.com
W: www.frost.com/equityresearch

Recent Highlights

Based on Allot's progress we assign an increased equity value of $473.6 million/1.63 billion NIS to the Company. We estimate Allot's stock price target to be in the range of approximately 43 NIS to 51 NIS with a mean of 46.85 NIS or 13.6 USD.

Allot generates revenues from two sources: (1) sales of Network Intelligence Solutions which show communication service providers what is happening on their networks at the highest resolution and allow them to control network traffic for a high quality experience for subscribers (2) sales of Network-based Security solutions, such as security as a value added service that communication service providers can offer to subscribers in order to protect them from cyber threats. These offerings solve major problems for communication service providers such as creating new streams of recurring revenue to deal with serious pricing pressures and allow providers to navigate the 5G ecosystem successfully.

Exploring the second quarter of 2020 indicates the following:

- Total revenues for the second quarter of 2020 were $32.8 million, an increase of 23% compared to $26.6 million in the second quarter of 2019.

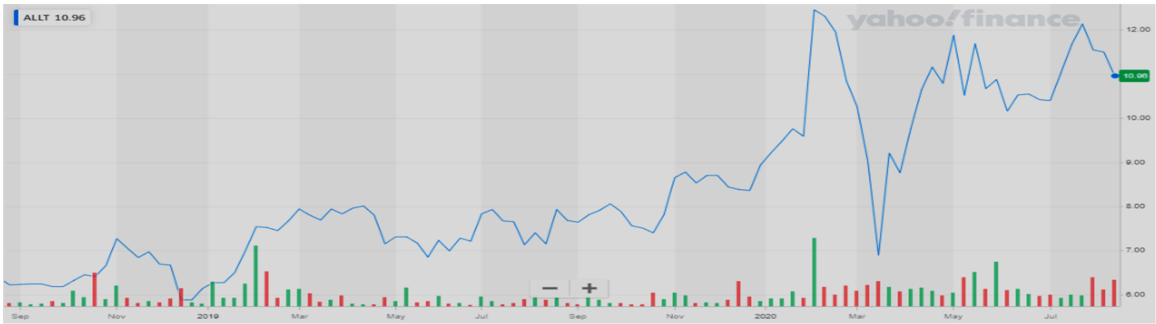
- Cash and investments as of June 30, 2020 totaled $109.2 million, compared with $110.7 million, as of March 31, 2020.

- Since the May 2020 first quarter earnings call, two recurring security revenue expansion deals were signed with existing customers

Read our annual initiation report below in order to get a comprehensive understanding of Allot's executive investment thesis, offering, market, competition, and growth drivers.

Forecast and Price Action:

000, $	2018A	2019A	2020E	2021E	2022E	2023E
Revenues	95,837	110,100	136,125	166,158	215,071	277,153
Gross profit	67,751	76,266	101,229	117,474	152,055	195,947
Operating (loss) profit	-4,810	-8,978	1,245	2,961	15,102	33,268

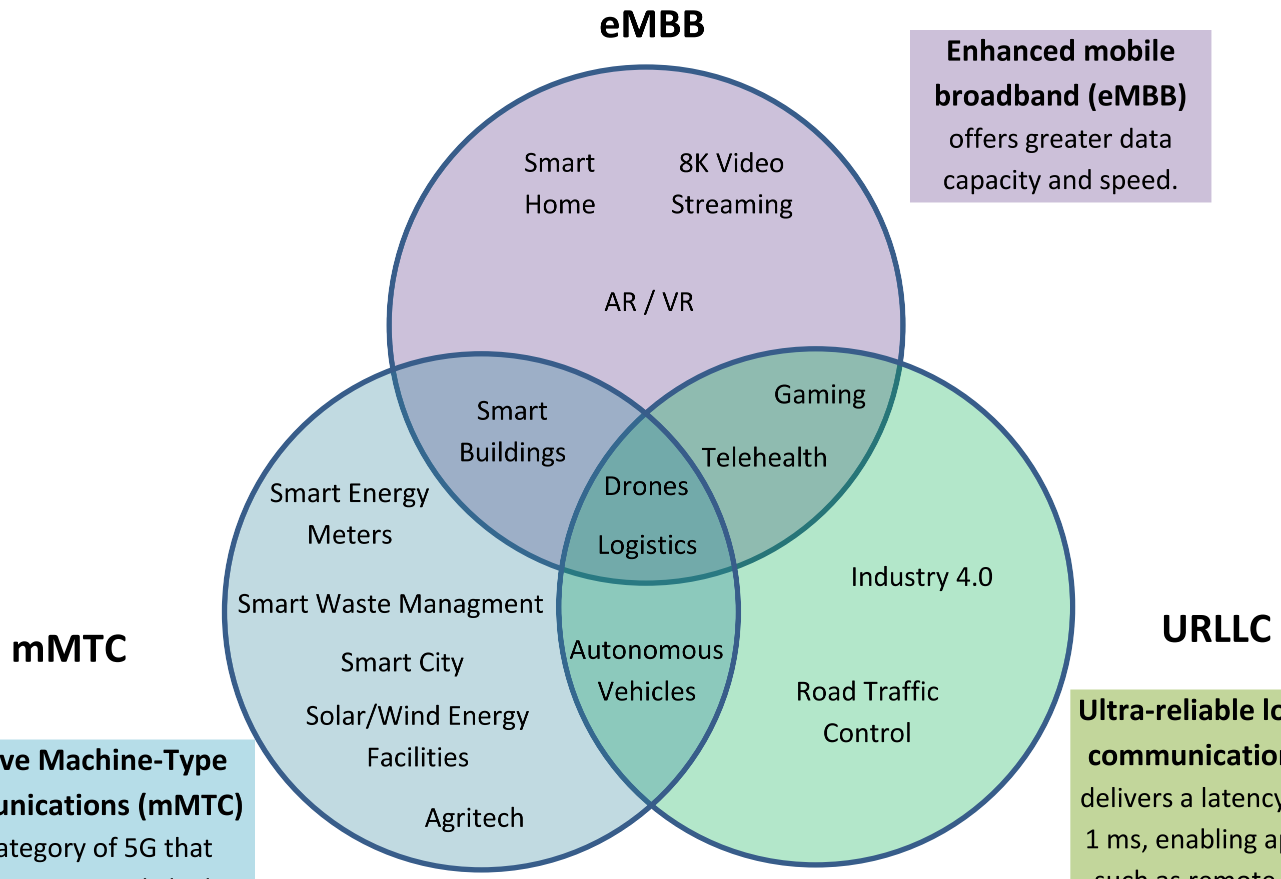


Executive Investment Thesis:

Today's forms of communication have made the world into a very small place. We can easily communicate with our families, friends, and colleagues, on the other side of the world, **via our cellular network,** to message them about the latest episode of our favorite Netflix show, streamed **via our home WiFi network**. Because these networks have become such a vital part of our lives they have become a vital asset for communication service providers (CSPs) that supply us with cellular, internet, and other services.

The problem is that as our **networks become more advanced to meet our expectations,** by supplying us with capabilities such as 8K video streaming, gaming, virtual reality, ultra-reliable low latency/low bandwidth V2X collision avoidance systems and other machine-to-machine communications on a massive scale, **we expect to pay less to use them**. That is, network costs are rising for CSPs but Average Revenue per User (ARPU) is not.

New Applications Empowered by 5G

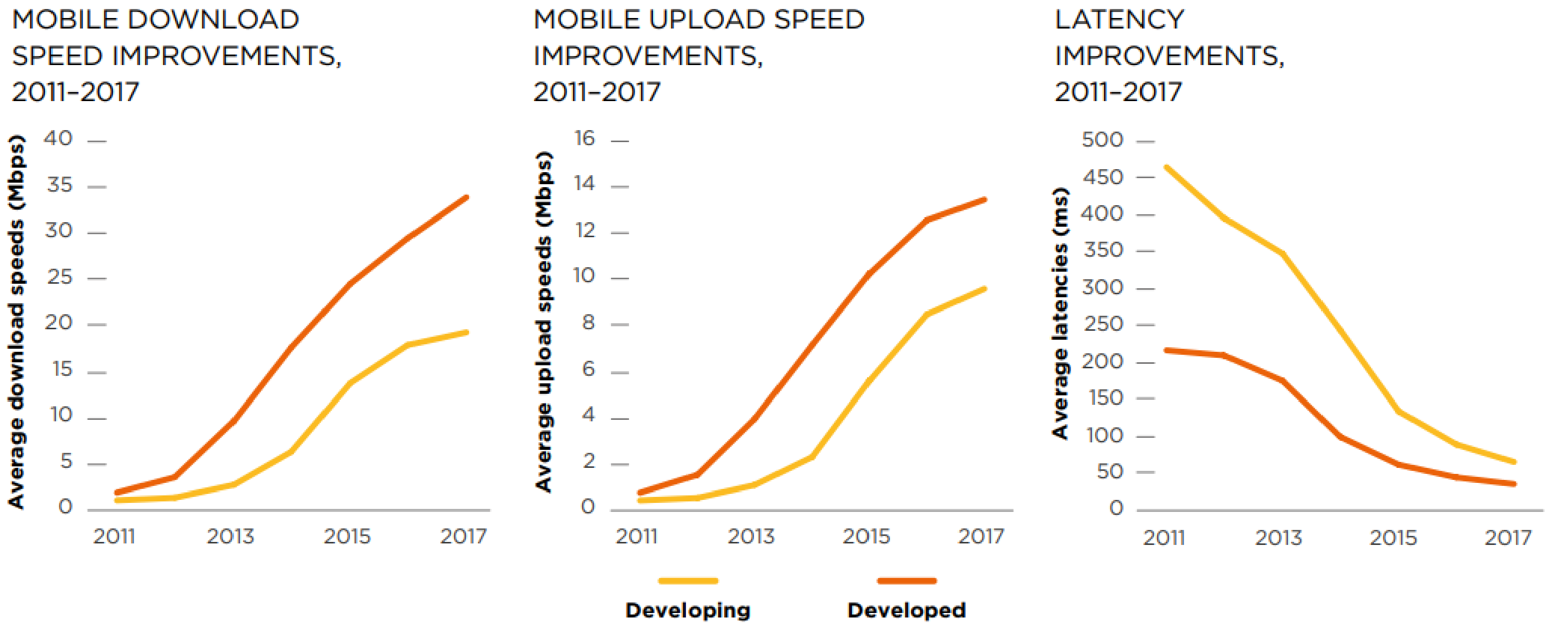


Enhanced mobile broadband (eMBB) offers greater data capacity and speed.

Massive Machine-Type Communications (mMTC) is a category of 5G that supports extremely high connection density of online devices. 10X more density than 4G LTE.

Ultra-reliable low latency communication (URLLC) delivers a latency of 5 ms to 1 ms, enabling applications such as remote surgeries, real-time gaming and V2V communications.

From the figures below it is evident that mobile networks have given users increasingly better download and upload speed as well as significantly improved latency but all the while have drastically dropped prices (both in developed and developing countries).

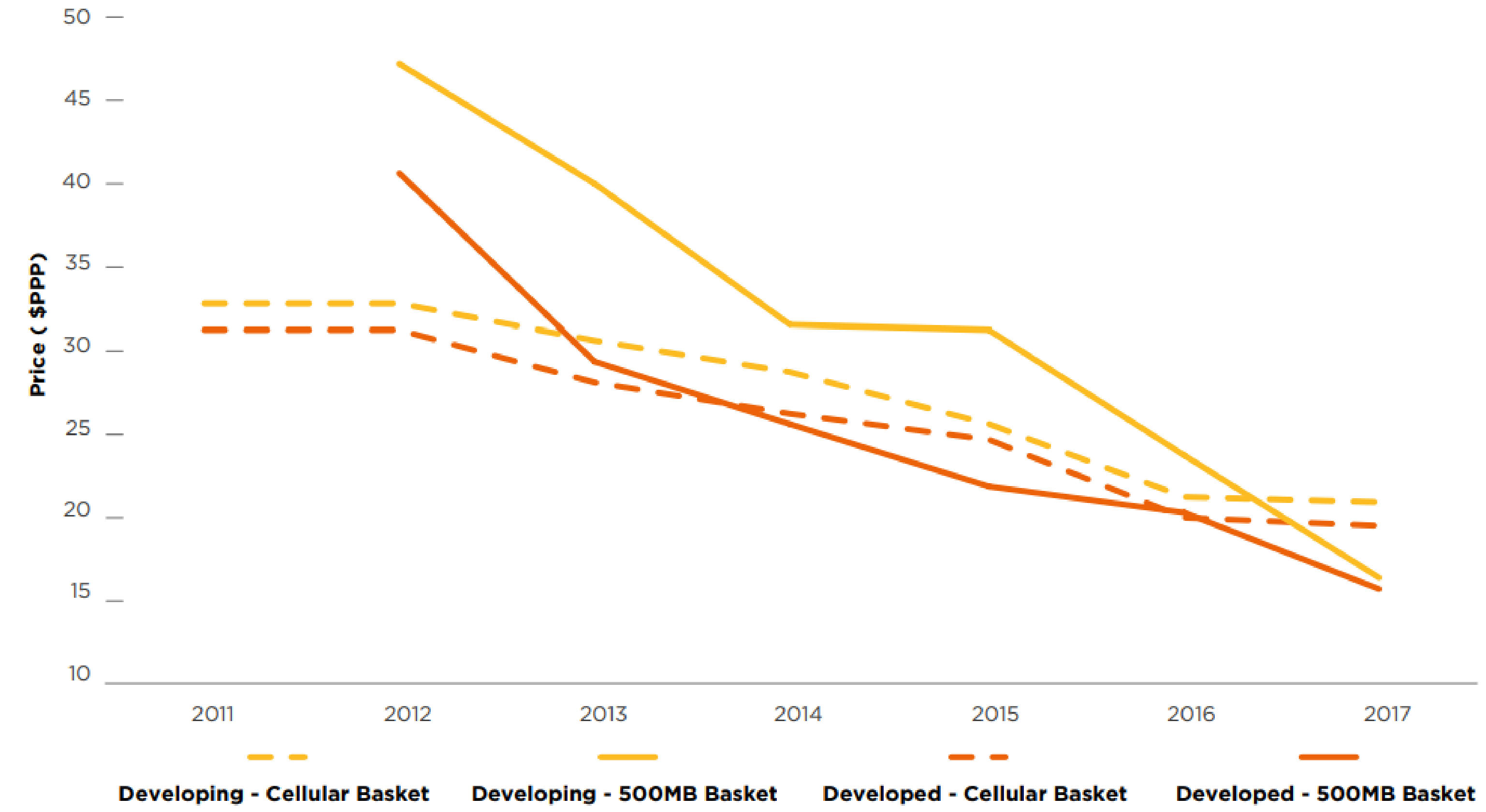


MOBILE DOWNLOAD SPEED IMPROVEMENTS, 2011–2017

MOBILE UPLOAD SPEED IMPROVEMENTS, 2011–2017

LATENCY IMPROVEMENTS, 2011–2017

AVERAGE PRICE TRENDS, 2011–2017



Source: GSMA Intelligence

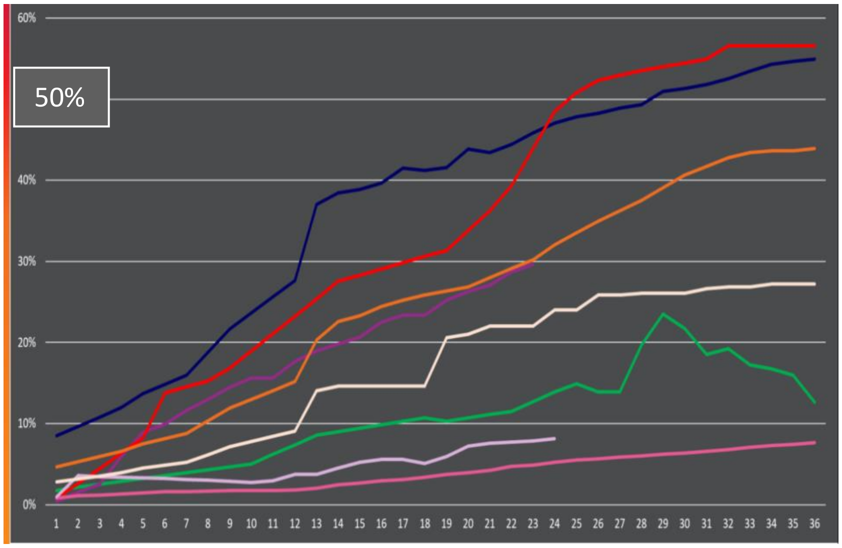
The second major problem that arises is that as more and more devices utilize CSP networks, there are more and more targets for cyber-attacks. Imagine a hacker infecting two million IoT devices and using them to launch a massive DDoS attack on vital city infrastructure.

The new Mobile Edge Computing (MEC) architecture of 5G networks only exacerbates this problem. Edge computing is a term to describe the migration of computing processes from a centralized cloud at the center of a network to a distributed cloud with nodes at the edge of the network, meaning, as close to the end user as possible. The edge computing nodes could be a local data center or even the user's device itself. The bottom-line is that there are many more points for attackers to target in the new 5G architecture.

So why are our networks migrating to a distributed architecture? This migration from a centralized computing entity to many small distributed computing entities on the edge of the network is happening for two reasons. The first is that as more and more devices connect to networks it becomes more expensive to support their needed capacity to communicate with one central cloud as opposed to many local distributed cloud entities. The second is that more and more applications are requiring ultra-low latency and this is significantly easier to achieve with computing nodes closer to the end user at the edge of the network.

The two major problems above- 1) **increasing data capacity pressure with increasing pricing pressure and 2) increased attack surface** are exactly the issues that Allot solves.

1) Increased Attack Surface- Allot attempts to turn the security problem into an opportunity for CSPs by creating an added source of revenue for them with their **Network Security** Solutions. If we think about it, we quickly realize that our homes have become mini IT organizations with at least 10 connected devices that surround us and that we surrender our most intimate details to. Because Allot's solution is network based (it is located on the CSP network) and not end-point based (the Company also provides end-point security where necessary) users do not have to download or install anything. They are automatically protected.



The graph to the left shows the subscriber penetration rates for Allot's security solution over months for different CSPs. We can see that gradually Allot's Network Security solution is achieving penetration rates of over 50% of subscribers of some cellular CSPs in certain geographies. Should CSPs communicate the need for this solution clearly and awareness develop with end users, the revenue potential for Allot is significant. Vodafone's (one of the largest Tier 1 CSPs in the world) CEO Vittorio Colao stated, "*Our Secure Net product (provided by Allot) is already generating 160 million in revenue… we have been building quietly and we will leverage on.*"

Allot has made a strategic decision to focus its marketing and sales efforts on Network-based Security reaching out to what seems like the blue ocean of cyber security. We expect Allot to show a significant increase in revenues over the next 5 years due to the high growth expected in this sector and importantly due to the company's transition from a CAPEX to a Rev-Share business model. The solution is offered in a SecaaS model and for every new CSP end user (subscriber) that chooses to secure their online experience, the CSP and Allot share the monthly user fee**. With each CSP servicing millions of subscribers the revenue potential of this value added service is great both for the CSP and Allot.** Allot is constantly onboarding Tier 1 and 2 telecom customers that offer Allot's security value added service to end users.

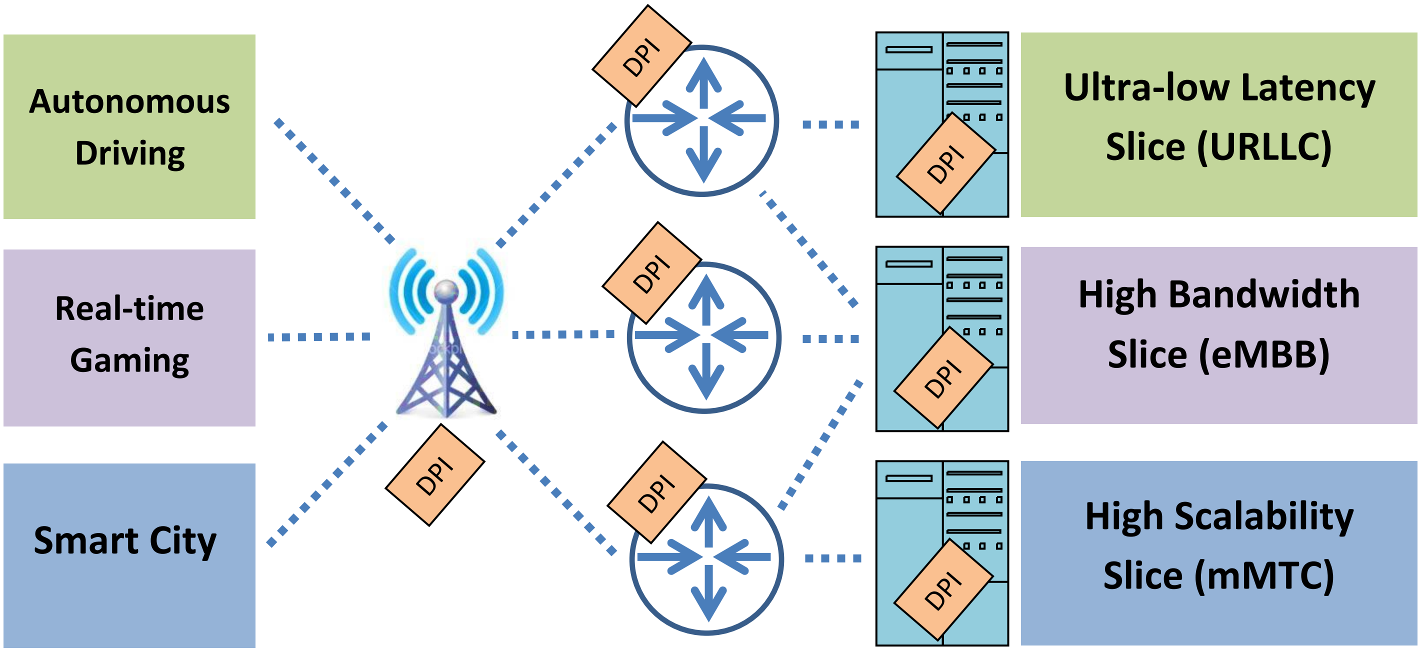
Allot's security solutions are also inherently designed to work well with the new 5G distributed architecture model. With the transition to mobile edge computing, large centralized computing clouds are replaced by smaller ones at the edge which are therefore highly sensitive to changes in bandwidth capacity. In relation to many of its competitors, Allot's solution sits inline with these edge computing nodes, meaning it does not take from their bandwidth and slow the network. Solutions such as those provided by Arbor/Netscout for example, send suspicous data to a scrubbing center which both takes up network capacity and costs more because of increased bandwidth for the CSP. Providing security solutions designed for 5G is critical for competing in this new market space. Thus Allot is well suited to address the challenges of 5G architecture and sees possible additional business offering focused securing the Network Infrastructure of the CSP itself from both inbound and "home-generated" attacks.

2) Increasing Data Capacity Pressure with Increasing Pricing Pressure- One of the cardinal challenges for CSPs is dealing with decreasing profitability in this new generation of communication networks. Tailored offerings have become crucial to providing added value to basic connectivity. In order to provide tailored services, CSPs need to have high resolution **Network Intelligence termed Network Visibility or Deep Packet Inspection (DPI)** in order to understand what data is flowing through their pipes and how they can capitalize on it. The higher the level of DPI sophistication, the more detailed a picture the CSP can obtain of the data flowing through their network pipes and in turn they are better able to act on this insight.

Allot's DPI solution provides insight that allows CSPs to get more out of their existing network bandwidth without intensive CAPEX investment from the part of CSPs. That is, simple broadband pipes, where data flows, become smart and sophisticated allowing CSPs to see what type of data is flowing and to adapt to points of congestion. By more efficiently using their existing infrastructure, CSPs are able to save significantly on CAPEX. In addition to this major benefit, Allot's solution also allows CSPs to offer a plethora of new services to customers such as parental controls, monetization (real-time data package offers based on user behavior), and most importantly, high Quality of Experience (QoE) to ensure that customers remain happy with their CSP no matter what their user behavior or application use case is.

In 5G, Network Intelligence or DPI are essential to meeting user needs. 5G by its very nature was designed to handle a wide variety of applications shown on the Venn diagram above. Each of these applications has unique requirements and therefore it is necessary for the data flowing through the network to be identified and categorized in order to meet these requirements. For example, data to stream an 8K video requires more bandwidth while data to perform a remote surgery requires ultra-low latency, and data to support smart utility meters requires high scalability but very little bandwidth, while data to support mobile banking requires high levels of security. The allocation of network resources to support these different market segments is known as 5G Network Slicing. Network slicing virtually slices networks from the core to the RAN (meaning throughout all parts of the network) in order to allocate resources for specific use cases. 5G Network slicing utilizes network functions virtualization (NFV) and software defined networking (SDN) to create different virtual networks on physical infrastructure. Network visibility or DPI is critical to 5G slicing to ensure Quality of Experience (QoE) analysis and management. This is also true from a security perspective; DPI allows identifying suspicious traffic patterns that could signal DDoS attacks or malware.

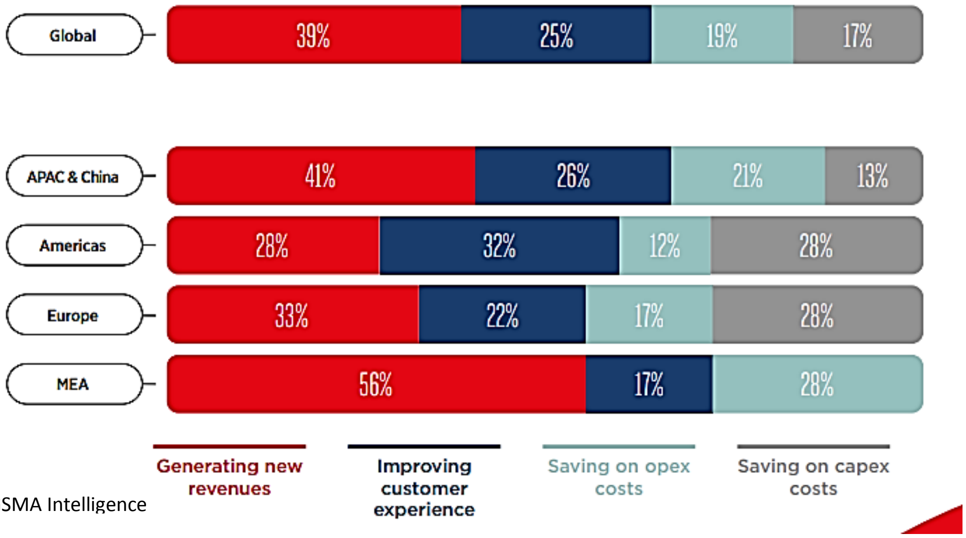
5G Network Slicing


Autonomous Driving
Real-time Gaming
Smart City
DPI
DPI
DPI
DPI
DPI
DPI
DPI
Ultra-low Latency Slice (URLLC)
High Bandwidth Slice (eMBB)
High Scalability Slice (mMTC)

In conclusion, Allot's DPI solution allows CSPs to 1) manage network traffic in order to relieve congestion and minimize CAPEX expenditure 2) ensure high QoE for users 3) enable policy creation and charging control such as parental controls and data usage limits 4) secure network traffic as an added revenue source for CSPs.

Revenue generation and customer experience prioritised over cost-cutting as the primary stimulus for network transformation

What is the primary goal driving your network transformation strategy? (% of respondents)



Source: GSMA Intelligence

In addition to 5G there are a number of other trends driving adoption of Network Intelligence and Network Security Solutions. These include the heightened use of networks during the COVID pandemic and the ever progressing regulatory landscape. **Under the 3GPP 5G standard it is mandatory for CSPs to have DPI capabilities.** Other regulatory policies strengthening Allot's offering include examples such as the UK introducing a law requiring all visitors of adult content websites to prove that they are 18 or over. This was done to reduce the risk of children accessing or stumbling into adult content and to set a standard for international child protection online. Sites that do not comply with the law will be blocked by mobile and fixed CSPs. Further regulations such as the implementation of the Network and Information Security Directive (NISD) and the General Data Protection Regulation (GDPR) in the EU that require network operators to ensure that their network and information systems meet minimum standards of cyber security could lead to significant upside for Allot.

Within the competitive landscape Allot is well positioned and provides network awareness and security of the highest quality. The nature of the company can be characterized to investors by its two offerings. The Network Intelligence solution brings in a constant and steady stream of revenues which according to our evaluation will show low two digit growth in the next two years and then transition to high one digit growth. The second offering, mobile Network Security, is a relatively new and growing business which we expect to have significant high double digit CAGRs in the next five years based on Allot's reputation, deep know how on a global scale, and the high potential of the Rev-Share model. Allot's main customer segment is telecom service providers which can leverage both of Allot's solutions. Due to the synergy between these offerings (one allows customers to see and control their networks and the other to secure them) we believe in the investment potential of the company.

Table of Contents

Executive Investment Thesis: 3

Company Overview: 10

Customers........ 12

Case Studies:........ 14

Competitive Analysis and Market Trends: 16

Competitive Analysis: Network Security 16

Competitive Analysis: Network Intelligence - Deep Packet Inspection (DPI)........ 18

Market Trends: Network Security 20

Market Trends: Network Intelligence - Deep Packet Inspection (DPI)........ 26

Financial Analysis:........ 33

Appendix A - Financial Reports........ 35

About Frost & Sullivan........ 37

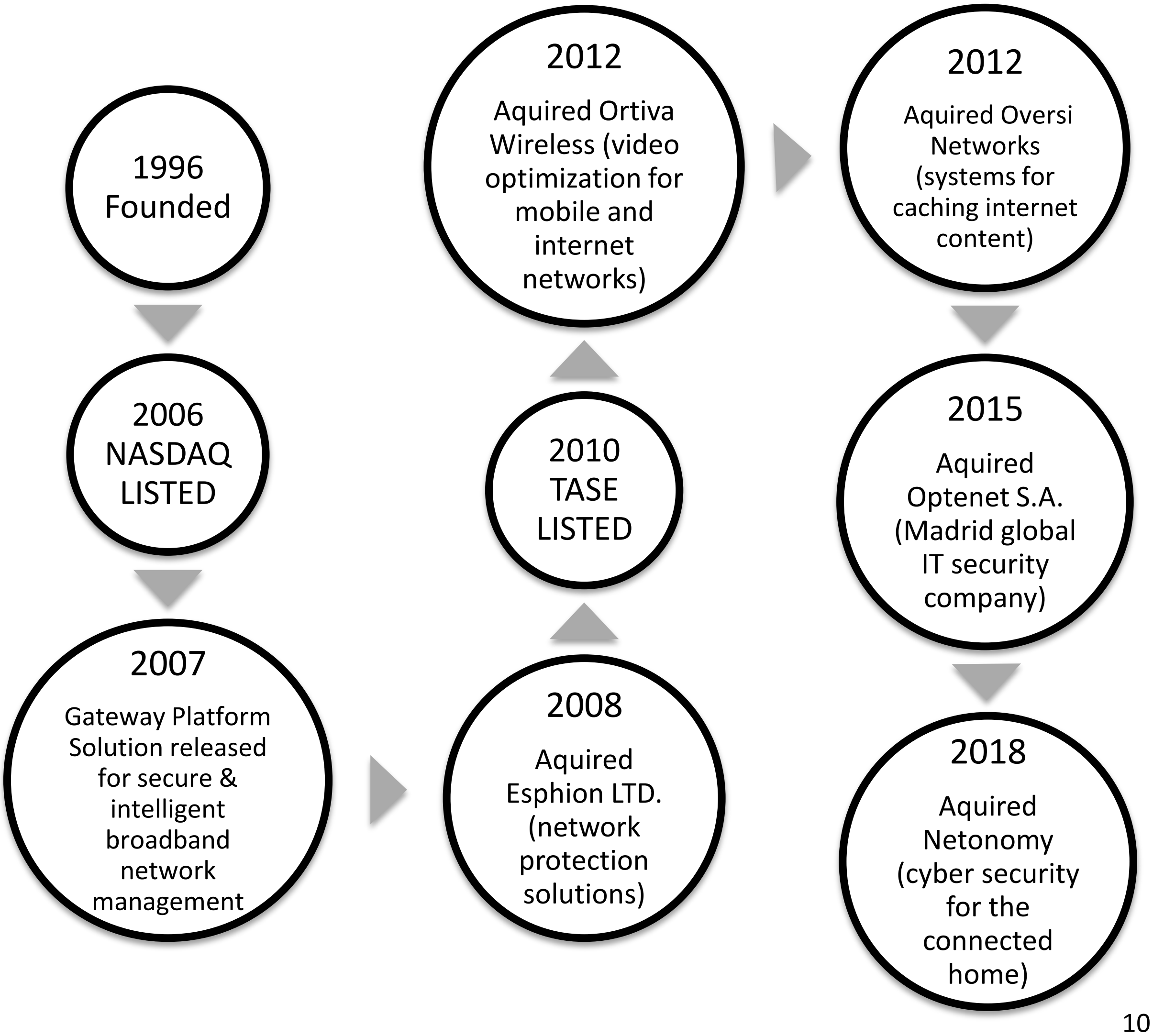
Disclaimers, disclosures, and insights for more responsible investment decisions........ 38

Company Overview:

Allot Ltd. (NASDAQ, TASE: ALLT) is a B2B2C software company with over 20 years of experience that focuses on 2 solutions:

1) Network security solutions
2) Network intelligence solutions

These solutions enable entities such as communication service providers (CSPs) to secure their networks and optimize the digital experience of their customers. Allot's motto is "See. Control. Secure." and it is a precise definition of the company's value proposition. The company allows its customers to see their network, control it to give the best personal experience to end users on all connected devices, and secure all of these devices against threats. It does this while providing network insights that save its customers significant capital and while creating new revenue streams for them. **In essence, Allot empowers its customers to get more out of their networks. A lot more.**


1996
Founded
2006
NASDAQ
LISTED
2007
Gateway Platform Solution released for secure & intelligent broadband network management
2008
Aquired Esphion LTD. (network protection solutions)
2010
TASE
LISTED
2012
Aquired Ortiva Wireless (video optimization for mobile and internet networks)
2012
Aquired Oversi Networks (systems for caching internet content)
2015
Aquired Optenet S.A. (Madrid global IT security company)
2018
Aquired Netonomy (cyber security for the connected home)

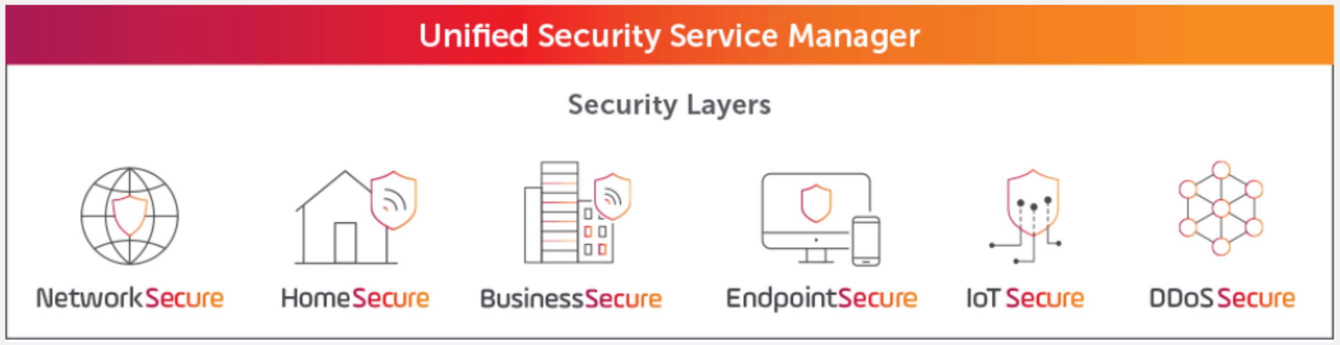
Since its establishment, Allot has acquired 6 companies including Esphion, Ortiva, Oversi, Optenet, and Netonomy. Allot has amassed a great deal of experience and know-how from their human capital, through their acquisition strategy, and through their experience designing and implementing use cases for large customers such as Reliance and Telefonica.

The company's HQ is located in Hod-Hasharon Israel where the principal administrative and research and development activities take place. Additional offices for either sales or research and development are located in the US, Spain, France, Italy, Singapore, South Africa, Columbia, and India.

Allot is network agnostic. Just as they secure and optimize mobile networks, they secure and optimize fixed, satellite, cloud and all other network types that support our connected devices such as laptops and IoT devices.

This means that their software turns broadband pipes into smart networks allowing value-added internet services to be rapidly deployed for Communication Service Providers (CSPs) of mobile broadband, wireless broadband, mobile satellite service, and digital subscriber line carriers. The two main platforms by which they offer their services are **Allot Secure** and **Allot Smart**.

Allot Secure is a network-based security solution intended to protect any and all connected devices from cyber threats. It consists of 6 parts (detailed in the chart below) that work together to achieve a unified experience. Allot Secure enables CSPs to offer security as a service (SECaas) to their subscribers. Revenue realized from Allot Secure is produced via a rev-share model between the CSPs and Allot.

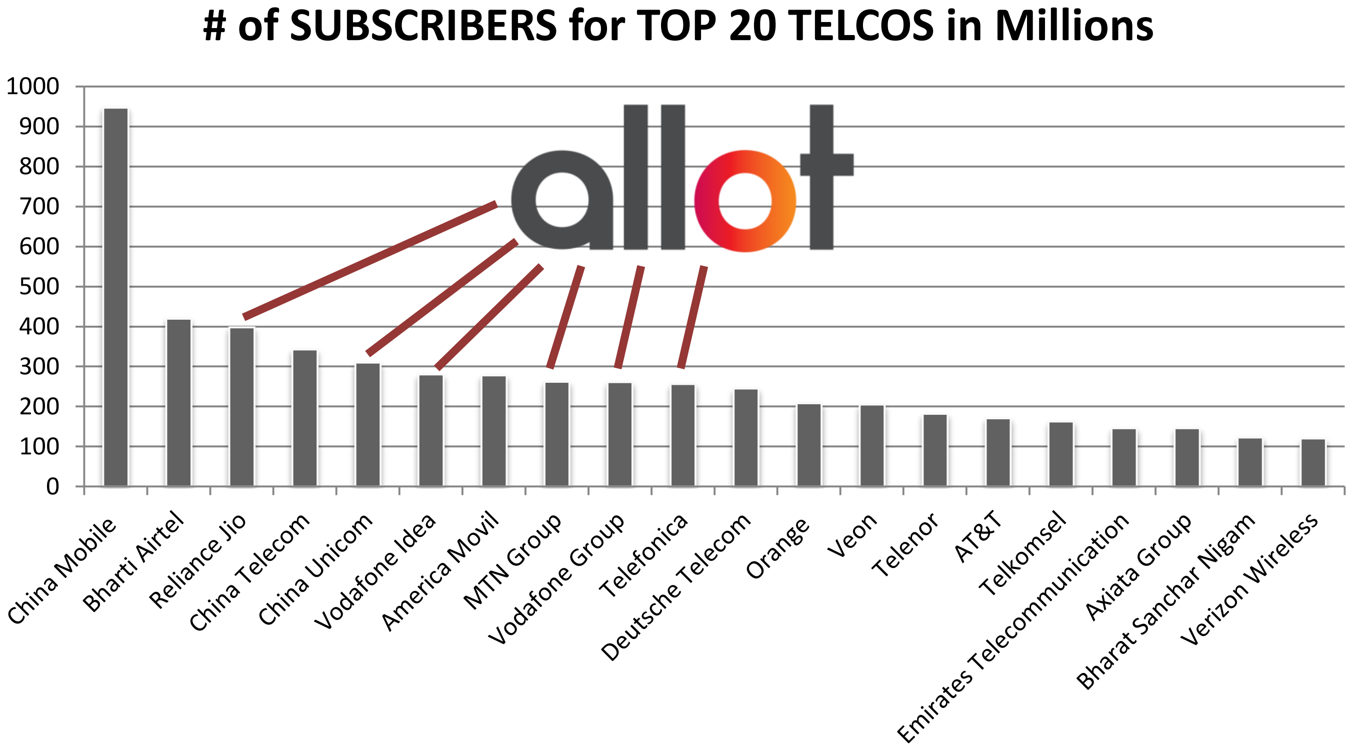


Allot Smart is a Network Intelligence or Network Visibility solution powered by deep packet inspection (DPI) technology that supervises and filters the data packets sent over the network. It enables a cost-effective high quality experience for users and has the potential to lower access bandwidth costs, defer bandwidth capacity expansions, and reduce revenue leakage. With Allot Smart a CSP can truly understand what type of data is flowing through their pipes, enforce policies such as parental controls or data limits, and perform network planning. For example, a CSP may choose to look at the changing trend in amount of YouTube users on their network, forecast future use, and understand that they are able to defer investing in capital intensive network infrastructure for a few years. An additional example would be a CSP having a congested network that does not deliver content at speeds and quality that create user satisfaction. Allot Smart identifies the sources of congestion in a network and mitigates the congestion delivering content that ensures a quality experience (QoE) and therefore limits churn.

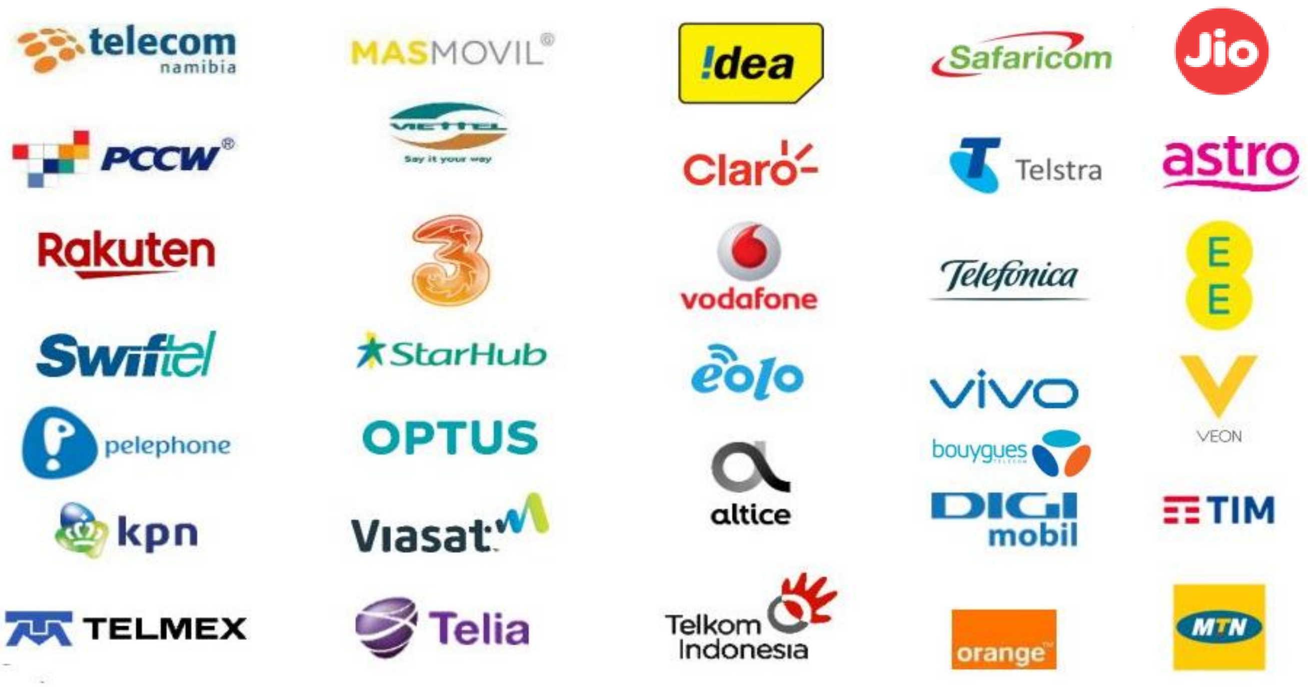
Customers

Allot solutions are deployed globally by the world's leading service providers and enterprises to improve network performance, ensure QoE, and deliver value added security services. Allot's combined customer base consists of 3000 installations and over 1 billion end users.

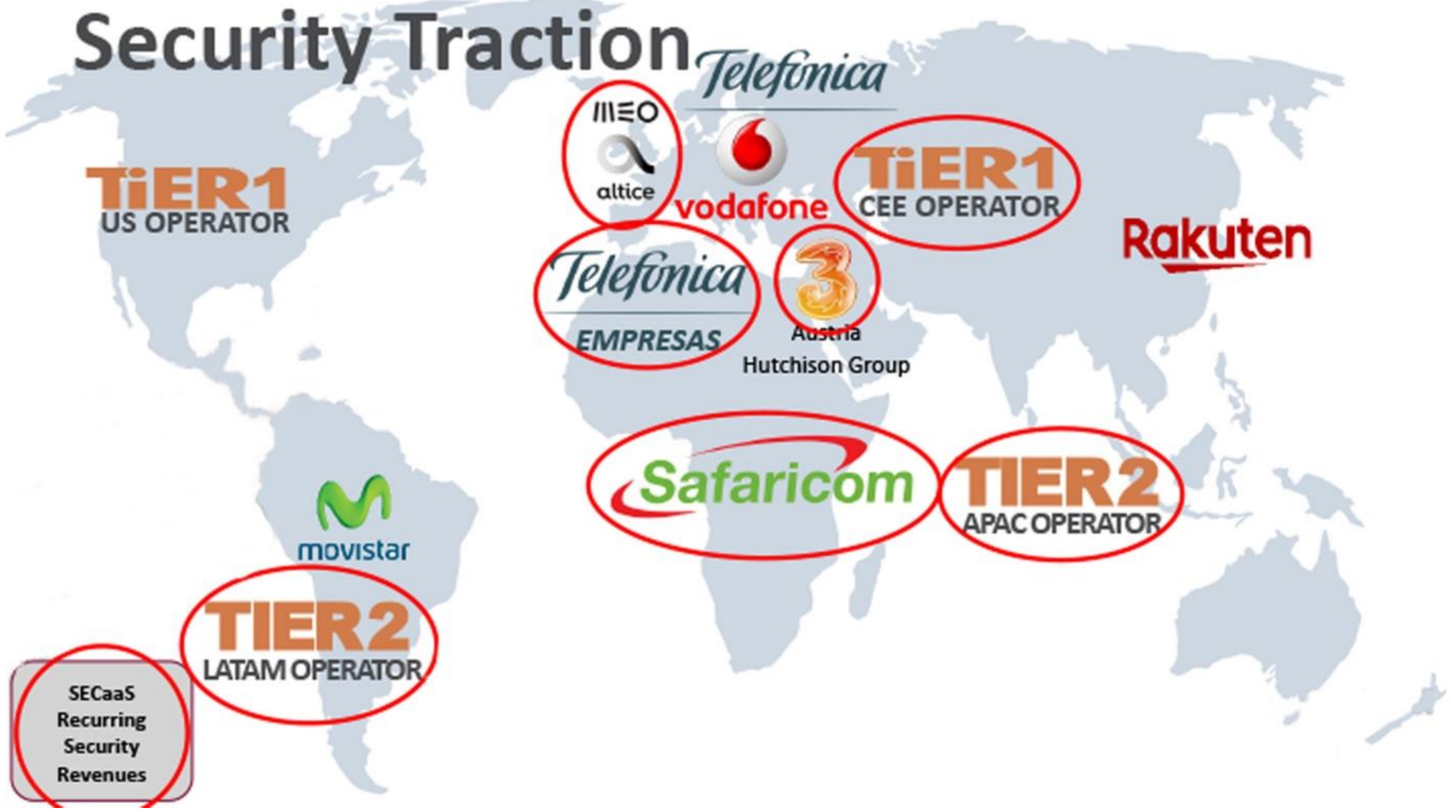
Allot provides its services to 13 tier 1 operators. The graphic below shows the largest mobile CSPs in the world by number of subscribers. Six of them toward the top of the list are publically verified Allot customers. For customer size comparison you can see that AT&T and Verizon are towards the bottom of the list. Allot also provides network intelligence and security solutions to enterprises. Customer breakdown is about 80% CSPs and 20% enterprises.



Some Allot Smart Customers Include:



Major Allot Secure Customers Include:



Case Studies:

❶ Safaricom

Vertical: Service Provider
Solution: Security
Region: EMEA

About Safaricom

Safaricom PLC is a listed Kenyan mobile network operator headquartered at Safaricom House in Nairobi, Kenya. With 29 million connections, they are the largest telecommunications provider in Kenya and one of the most profitable companies in the East and Central African region. The company offers mobile telephony, mobile money transfer, consumer electronics, ecommerce, cloud computing, data, music streaming, and fiber optic services. It is most renowned as the home of MPESA, a mobile banking SMS-based service.

Challenge

- Need for parental control and anti-phishing/anti-malware capabilities
- Interest in monetizing and differentiating in the SECaaS market
- Optimize data analysis of vast amounts of traffic on networks

Solution

Safaricom adopted the Allot Network Secure solution. This solution powers Safaricom's "Secure Net" giving them the ability to offer their customers a unique Security Service that protect users from prevalent cyber threats, like harmful websites and applications, virus downloads, and malware. In addition, rumors of parental control regulation in the region have been circulating and the operator wanted to be prepared by rolling out parental control functionality to their customers ahead of the official regulations. This solution allows Safaricom end-users to enforce parental controls. The addition of this feature also serves as the operator's entrance to the SECaaS market. Safaricom is the first network operator to introduce these security services in the region, which helps to differentiate them from the rest of their competition.

❷

Vertical: Service Provider
Solution: DDoS Protection and
Congestion Management
Region: EMEA

About VOO

VOO is the leading provider of broadband cable services in southern Belgium. VOO delivers digital TV, telephony, and high-speed Internet service at 50, 100 or 150 Mbps.

Challenge

- Infrastructure expansion was not a sustainable strategy due to high cost
- Cable connectivity is highly vulnerable to congestion
- Lack of visibility into the network prevented optimization

VOO's growth trajectory and ability to attract new customers and keep them, depends on the operator's ability to deliver non-stop access with consistently good quality of service. As a shared media, cable connectivity is highly vulnerable to congestion. VOO's fast expansion was challenged by frequent and unpredictable episodes of congestion mainly on upstream channels which have limited capacity and could not accommodate the bandwidth demand. While preliminary investigation led VOO to suspect P2P traffic as the main cause of the recurring congestion, the operator was lacking the network visibility to validate this assumption. In addition, some congestion episodes were so extreme, they completely disabled service delivery, impacting tens of thousands of customers. VOO needed a solution that could pinpoint the cause of the congestion and control it cost-effectively, in compliance with net neutrality guidelines.

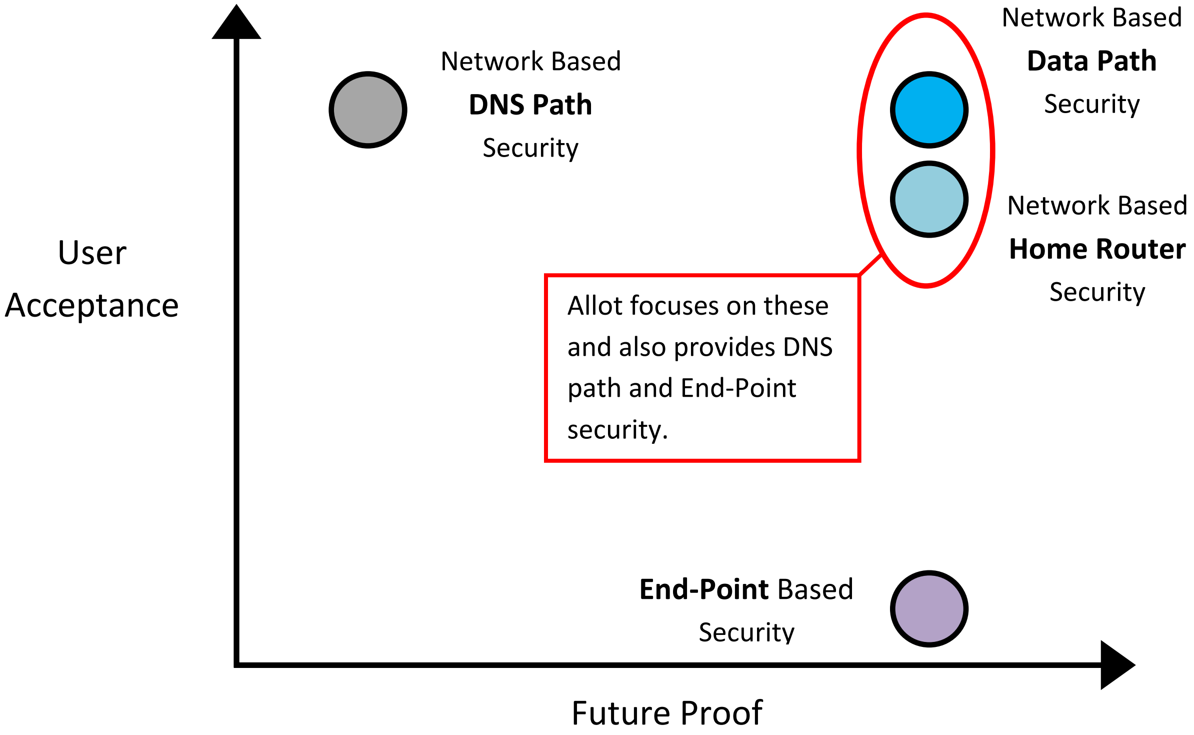
Solution

The Allot Service Gateway was deployed giving VOO full visibility of network traffic per CMTS channel or bonding group. As a result, VOO can see and manage all traffic on the network at a granular level, all from a central vantage point. Instead of controlling CMTS policy based on IP subnets, which can affect an entire residential neighborhood, VOO can enforce QoS policy on a discrete saturated node(s) that affects only one street in the neighborhood. The granular traffic visibility provided by Allot showed VOO that 10% of CMTS upstream bonding groups were congested and confirmed that the culprit was P2P traffic which consumed 80-90% of the upstream bandwidth. VOO was able to reduce congested bonding groups from 10% to 1% almost immediately, which freed up bandwidth for other services and delivered higher QoE for end-users. VOO also activated Allot's DDoS protection service (DDoS Secure), which is fully integrated in the Allot Service Gateway. The activation revealed that the unpredictable service disruptions were indeed caused by massive DDoS attacks. Once the Allot DDoS Secure sensor VOO is now recognized as the best performing network for delivering Netflix video content in their region. VOO is able to postpone investment in infrastructure expansion by 2 years.

Competitive Analysis and Market Trends:

Competitive Analysis: Network-based End-User Security

Security Method Mapped by User Acceptance and Future Relevance



Competition within the Network Security domain can be split into four major categories:

1) Network based Data Path: security that is located in the network itself and not on our devices which inspects data going through the network 2) Network based DNS path: security that keeps users away from known malicious website domains 3) Network based Home/Business Router: security that is present on home or business routers 4) End-Point: security that is downloaded onto our devices themselves.

We mapped these categories on two axes: 1) User Acceptance and 2) Future Proof.

End-Point security is highly future proof but it is not user friendly because end users do not tend to download it on their mobile devices (the penetration rate is about 2%) let alone update it.

The Domain Naming System or DNS is a methodology by which a domain name is translated into an IP address where our webpage data is located. This system is put in place simply because we are people and for us it is easier to use words to name our websites and not numbers. For example, when we type in "YouTube.com" in our web browser the DNS is what translates this into a numbered IP address that retrieves the correct data from YouTube. DNS based security inspects domain name requests before fulfilling them. If the DNS request is for a known malicious domain, such as a phishing website, or its content is categorized as inappropriate by a parental control service, the user is redirected to safety. However, this approach faces a few problems.

Writers of malware avoid the use of DNS, only a minute fraction uses DNS for payload download. A second issue is that children easily avoid DNS-based parental control with apps like Google/Jigsaw that open an encrypted tunnel to the Google DNS system, circumventing the CSPs system without any remedy. A third issue is that DNS security is not relevant for IoT security and the connected home.

As opposed to DNS-based systems, network-based Data Path security inspects all data packets including DNS and HTTP/S and cannot be bypassed. It too redirects the user to safety if the domain in question is known to be malicious or its content is categorized as inappropriate.

But network-based Data Path security also faces a challenge. Encryption not only hides the consumer's personal data, it also hides malware and viruses from detection. Data path solutions need to be sophisticated and apply techniques such as ML in order to identify encrypted malware packets. Unlike DNS-based security, network-based Data Path security cannot be bypassed and despite the wide adoption of encryption, anti-malware engines are still effective. The evidence points to a network based Data Path security solution being an option of the highest quality and efficacy to protect the mass market against the growing threat of cyberattacks.

Network-Based -Data Path	**Network-Based -Home Router**
•**Perceived Strength**: "best functionality", Future proof, high penetration •**Perceived Weakness :** long integration, cost of solution scales with traffic increase •**Players**: Allot / Fortinet / Palo Alto (SMB) **The areas where Allot is very strong compared to its competitors are in 1) engagement with the end customer, 2) scalability, and 3) unification. These are areas that were developed through extensive work with Tier 1 providers such as Vodafone and come from a real need of CSPs.** **1) Many of Allot's competitors are B2B players. Allot is a B2B2C Player and therefore they provide engagement tools that CSPs can use to engage end users. These include campaign management tools that gradually onboard end-users through try and buy security campaigns as well as provide them with reports that show them the efficacy of being protected. This**	•**Perceived strength**: IoT visibility and protection; per device protection •**Perceived weakness**: slow adoption due to CPE legacy variety; •**Players**: Allot / SAM / Trend-Micro / F-secure / McAfee / Cujo **The areas where Allot is very strong compared to its competitors are 1) Security can run on legacy routers because it has a low signature and high performance. 2) Allot knows to check for viruses (as opposed to only malware) 3) They provide high resolution analytics to both end-users and CSPs to show them what is happening in the home network 4) Allot's solution is a unified solution. This means that not only can they protect our routers, they can protect our phones, and all other connected devices inside and outside of the home. This means that if a parent sets parental controls on their child's devices, these controls are effective when the child is using the home WiFi network or when they are using the mobile network outside of the home.**

significantly increases penetration and such campaigns can target millions of users at a time. **2) Allot is strong in the area of scalability. Its solutions are designed to scale to millions of subscribers which is an area that is difficult for many competitors** **3) Allot's solution is a unified solution. This means that not only can they protect our phones, they can protect our routers, and all other connected devices inside and outside of the home. This means that if a parent sets parental controls on their child's devices, these controls are effective when the child is using the home WiFi network or when they are using the mobile network outside of the home.**	
Network-Based -DNS Path •**Perceived strength**: simplicity for fixed networks; "good enough" •**Perceived weakness**: easy bypass by users; bypass by Google –not future proof to DoH; fail to solve majority phishing attacks, no virus protection, no IoT protection •**Players**: Akamai / Infoblox / Cyan **Allot does not rely on DNS Path Security but provides it.**	**End-Point Based -Applications** •**Perceived strength**: complete functionality; protects anywhere •**Perceived weakness**: low penetration (the fact that actively downloading this solution is necessary causes a major drop in adoption rates) •**Players**: McAfee / Bitdefender / Kaspersky / Symantec (Broadcom) / F-Secure **Allot works with McAfee and BitDefender to provide End-Point Security**

Competitive Analysis: Network Intelligence - Deep Packet Inspection (DPI)

DPI is simply a term to describe inspecting the packets of data that flow through a network. When these packets are identified by type, this allows CSPs to know exactly what is going on in their network as well as to act upon it. For example if a parent does not want their child to have access to certain content, a DPI solution identifies that this content is going through the network and then blocks it from entering the child's phone. Accurate data traffic classification is essential for achieving visibility on networks so that network operators can make the best decisions about traffic management. But when data is encrypted this is very difficult to achieve. The best DPI solution is one that knows to identify the largest amount of types of data at the highest resolution while circumventing encryption of data packets. For example a basic DPI solution would be able to identify that a packet of data is in general Facebook content, whereas a sophisticated DPI solution would be able to identify what type of Facebook content exactly is going through the network (a message, a video message, etc.), set very specific controls over which type of data is allowed to go through, and furthermore, learn what is being done to try and bypass the controls it put in place. Things the DPI learns from one device can be shared through the network to apply to all devices. These features of an advanced DPI are what allow deep insights for CSPs and high QoE for users and they require very deep know-how and experience. Allot has all of the features of a sophisticated DPI.

The DPI market can be roughly segmented into two types of players: 1) **Pure players**, which include only Allot and Sandvine, 2) **Network Equipment Providers (NEPs) with a DPI feature** such as Huawei, Cisco, or Nokia.

Pure players offer a holistic DPI solution that not only understands what data is flowing through the network but that also allows control of data flow for automated congestion mitigation, policy enforcement such as parental controls, or 5g slicing (allotting only parts of a network to deliver 5g capabilities as not to burden the whole network).

Sandvine and Procera merged in 2017 to create a strong competitor (Sandvine) in the DPI market. The resultant portfolio addresses customers' needs for analytics, policy charging and control, traffic management, security, regulatory compliance, and cloud managed services. Its addressable market also targets growth opportunities of 5th generation wireless networks, Internet of Things (IoT), software-defined networks (SDN) and network function virtualization (NFV). The Sandvine and Procera joint client portfolio represents more than 2.5 billion subscribers and 500 network operators. Before the merger each of these 3 players owned about one third of the pure play market, resulting in Sandvine now having a 2/3 market share.

NEPs with a DPI feature also provide a holistic solution but, because DPI is not their main offering the resolution of visibility into what is happening in a network along with the ability to control the network are not close to the level of pure players. However, these solutions may be cheaper especially if a CSP has purchased infrastructure from the NEP. In addition, under 5G, it has become obligatory for NEPs to provide basic DPI functionality. Aside from the lack of expertise and resolution in providing DPI solutions, NEPs do not provide inline DPI solutions like Allot does. This means the solutions they provide take up bandwidth and slow the network down as well as increase costs for the CSP.

Allot's DPI fits all the criteria of a sophisticated and advanced DPI:

1) It offers multi-dimensional **Network Awareness** (visibility of what types of data is flowing through a network) on one of the highest levels in the industry. Allots solution allows customers to by-pass encryption so that they can best manage traffic and confidently assure network efficiency, quality of service and users' quality of experience. It does this via ML, which proactively learns and adapts to the changing tactics of services and applications that use encryption. Allot's synergy of inspection methods results in highly granular and **accurate recognition even at maximum speeds and peak loads.**

2) It uses **ML and AI** to ensure QoE by prioritizing data that is most crucial to satisfy customers in order to limit customer churn.
3) The level of customization of policies that can be enforced on a network create **flexibility** that is on one of the highest levels in the industry. In addition to policy enforcement this gives the ability to deploy personalized service plans for individuals and groups and to evaluate the performance of tiered and quota service plans.
4) Allot's DPI, **by nature, is designed to meet the specific needs of CSPs. This is due to the Company's extensive work with CSP throughout the years.**
5) The solution is designed as a **service gateway** which means that other critical services can be laid on top of it seamlessly. This includes firewalls, analytics tools, and caching.
6) The Allot solution enables CSPs to **comply with local regulations**. It blocks illegal content such as pornography, violence, drugs, child abuse, fake and untruthful content and illegal applications. It is specifically designed to enable CSPs to meet national law enforcement and/or homeland security authority requirements.

All of these advanced DPI capabilities allow CSPs to:

- Save access bandwidth costs
- Defer capacity expansion
- Cut OPEX through automation
- Reduce revenue leakage
- Prioritize network traffic
- Optimize and sustain peak user QoE
- Decide on future network investments
- Evaluate the viability of potential new offerings for boosting service uptake
- Segment and target subscribers
- Create subscriber profiles based on usage patterns
- Virtualize their networks and adapt to tomorrow's needs such as 5G slicing

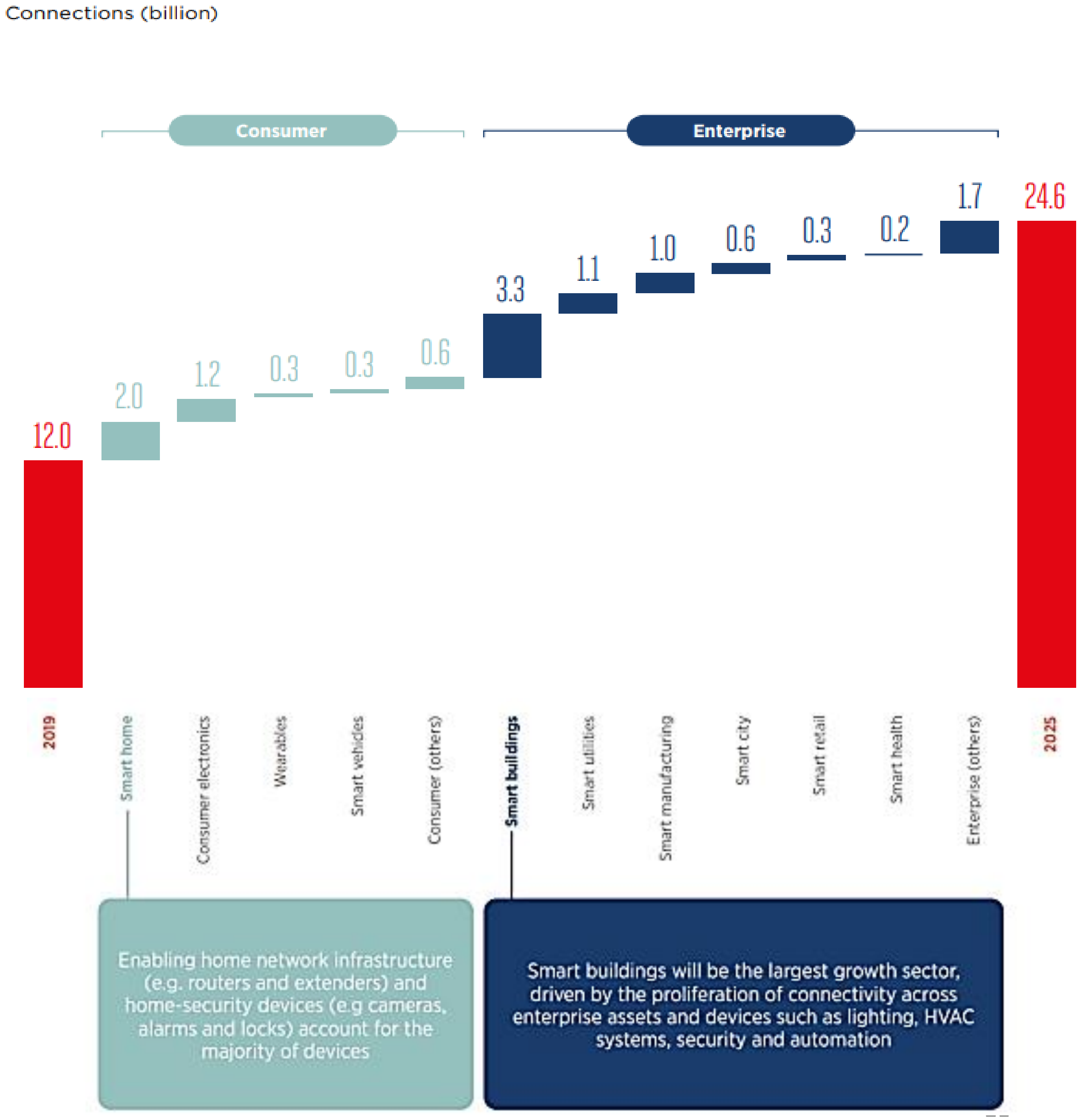
Market Trends: Network Security

The plethora of connected devices, connectivity protocols and applications enable unprecedented access to and transfer of data and information. As the dependence of consumers and enterprises on networks for myriad requirements grows, so does their vulnerability. Attacks can cost millions of dollars, impact competitiveness and damage reputation of companies which increases customer churn. The high complexity of systems and networks enhance vulnerabilities making the task of securing them even more challenging.

Network security utilizes software and hardware technologies to maintain integrity, confidentiality and accessibility of networks and data. Effective network security can thwart unauthorized access and stop a variety of threats from entering the network via policies and controls implemented across multiple layers at the edge and in the network.

With the implementation of the Network and Information Security Directive (NISD) and the General Data Protection Regulation (GDPR) in the EU in 2018, operators must ensure that their network and information systems meet minimum standards of cyber security. Multiple incidents and vulnerabilities reported in recent times targeting communication service providers mandate proactive response plans and tools to deal with legal, operational, technical, reputational and regulatory risks. CSPs with their core infrastructure and the large volumes of personal data they hold on subscribers, become target for malicious incidents. With Allot's solution, CSPs can both protect their own network infrastructure and offer value added Security as a Service (SECaaS).

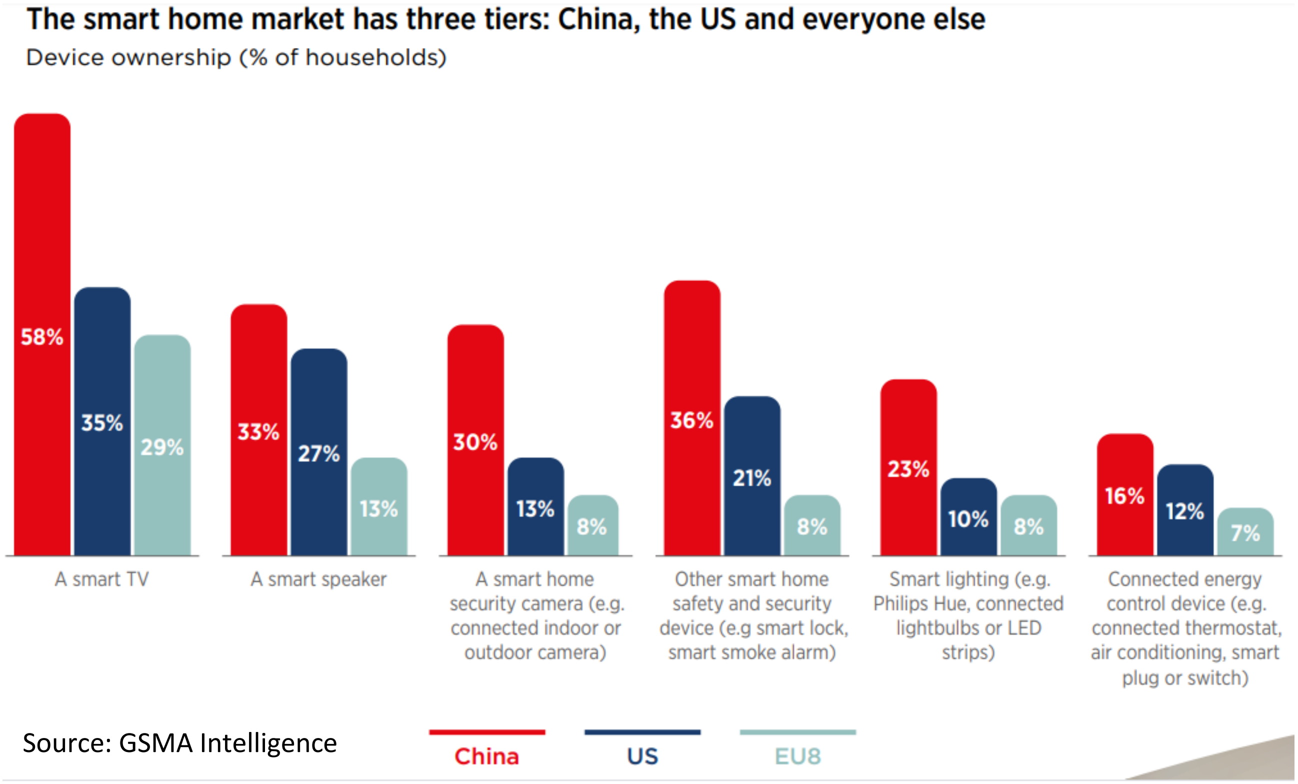
There will be around 13 billion new IoT connections by 2025; smart buildings and smart home are key growth verticals



Enabling home network infrastructure (e.g. routers and extenders) and home-security devices (e.g cameras, alarms and locks) account for the majority of devices

Smart buildings will be the largest growth sector, driven by the proliferation of connectivity across enterprise assets and devices such as lighting, HVAC systems, security and automation

Source: GSMA Intelligence



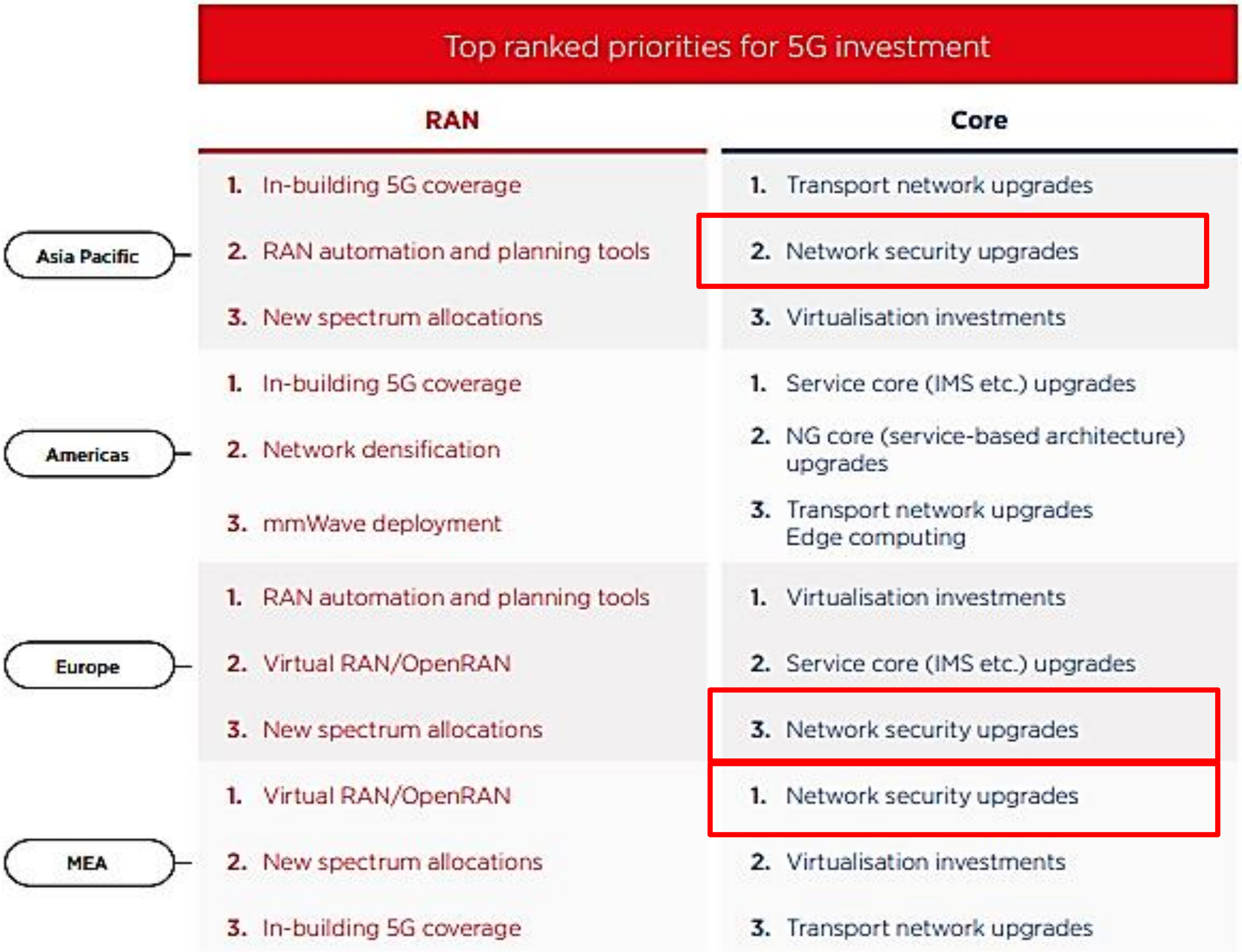
The smart home market has three tiers: China, the US and everyone else

Device ownership (% of households)

Source: GSMA Intelligence

Trends Impacting the Network Security Market

1. **Zero-trust approach to network security**—the zero-trust approach has moved beyond being a buzzword and with BYOD, cloud computing, and remote workers, its adoption will soon be mandatory as a network security best practice. Insider threats are occurring in alarming proportions and devising methods to mitigate these is the way forward.
2. **Enterprise mobility changes the requirements**—Emergence of the BYOD trend and "work from home" are directly related to an increase in enterprise mobility as companies adjust to employees' preferences for smartphones, tablets, and portable computers. The network security framework and solutions undergo changes to meet BYOD enabled workplaces. Network security solutions must be flexible to adapt to different operating systems, hardware and software.
3. **Advanced technologies in network security**— AI and ML-enabled network security systems enhance existing defense capabilities and over time 'learn' to identify unusual patterns and malicious activities. This helps to detect and stop known threats. The real value is however when encrypted web traffic can be monitored for unseen variations of known threats or related new threats or new malware threats. Automatic alerts regarding unusual patterns to security teams increase the effectiveness of the system by dealing with skills and resource gaps.



Top ranked priorities for 5G investment

	RAN	Core
Asia Pacific	1. In-building 5G coverage	1. Transport network upgrades
	2. RAN automation and planning tools	2. Network security upgrades
	3. New spectrum allocations	3. Virtualisation investments
Americas	1. In-building 5G coverage	1. Service core (IMS etc.) upgrades
	2. Network densification	2. NG core (service-based architecture) upgrades
	3. mmWave deployment	3. Transport network upgrades Edge computing
Europe	1. RAN automation and planning tools	1. Virtualisation investments
	2. Virtual RAN/OpenRAN	2. Service core (IMS etc.) upgrades
	3. New spectrum allocations	3. Network security upgrades
MEA	1. Virtual RAN/OpenRAN	1. Network security upgrades
	2. New spectrum allocations	2. Virtualisation investments
	3. In-building 5G coverage	3. Transport network upgrades

Source: GSMA Intelligence

Factors Driving Adoption of Network Security

The exponential increase in connected devices and consequently the increase in data and information that networks have access to, mandate the presence of comprehensive security.

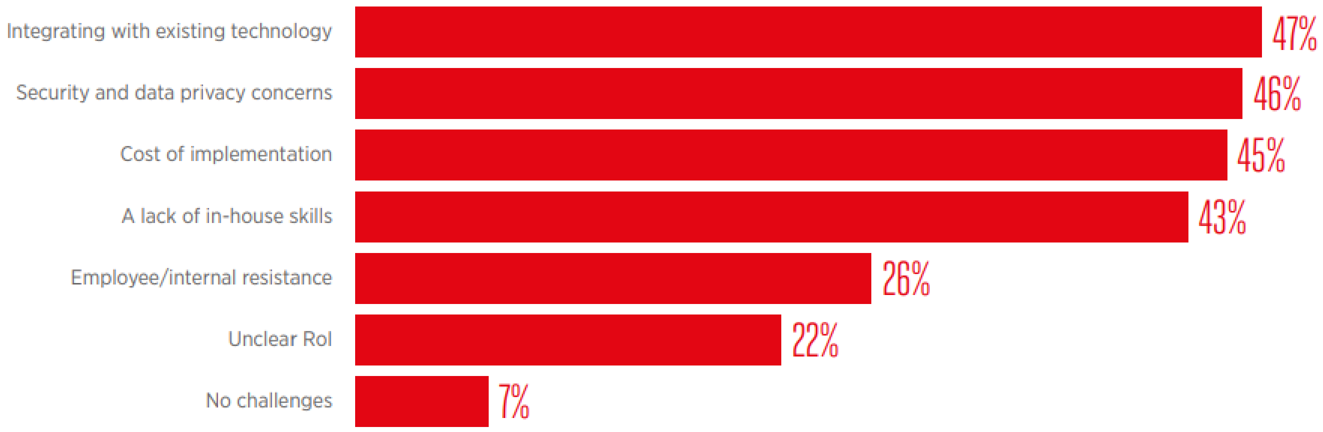
Major Drivers Impacting Adoption of Network Security	
Transformation in Telecommunication and other industries	In addition to the increasing number of mobile and connected devices, digital transformation in industries is also led by the adoption of other technologies such as Cloud, AI and ML. This increases the complexity of the network, and with multiple end-points, hybrid cloud structure, single-layered security architectures are ineffective, leading to the adoption of multi-layered, and comprehensive network security.
Privacy concerns	As more customers and their devices become part of the network, data and information flow have increased considerably. This makes it imperative that network security is notched up further to meet the demands of maintaining data security and

	privacy.
Regulatory changes	The evolution in communication, access to data, and information in the network has made regulators take notice of the risks of breaches. This has led to implementation of stricter norms and guidelines that companies must adhere to in order to ensure that they adopt best practices in securing the data of their customers.
Constantly evolving security hacks	Potential hackers are aware of the increase in surface area to attack network security. Technologies such as AI and ML are being used by hackers to constantly evolve and introduce new threats. New users, unaware of the need to implement adequate security measures are easy targets using a multitude of channels such as emails, apps, etc.
Additional layer of security	End users understand the importance of implementing security features; however, lack of knowledge and best practices are deterrents.

Source: Frost & Sullivan

Integration with existing technology and security concerns persist as main challenges

Which of these challenges does your organisation face in deploying IoT-based solutions? (% of respondents)



Source: GSMA Intelligence

Operators could offer managed security services as part of a broader IoT contract, relieving enterprises of the skills gap and costs to do so themselves

Factors Constraining Adoption of Network Security

Lack of standardization and fragmentation creates confusion among users. While they look for integrated products and services, network providers need to find partners in the ecosystem with similar goals and approaches when it comes to importance of security.

Major Constraints Impacting Adoption of Network Security	
Lack of unified network security	Fragmentation in the market confuses users and they end up with implementing inadequate network security. Lack of comprehensive solutions that can meet a variety of needs creates significant gaps that can be harmful to networks. The solutions must be able to scale up and meet the ever increasing and evolving needs of networks.
Security budgets	Implementing network solutions requires consistent updates and changes. This requires companies to invest in network security, which may not always be feasible. On the other hand adopting advanced network security solutions takes some of the load off of organizations to hire IT professionals.
Lack of standardization	Different systems and protocols may not support integration of different providers and APIs to create a comprehensive system. Users may not be able to make configuration changes leaving vulnerable areas in the network. Devices may use completely different systems making visibility and management difficult.
Lack of trained professionals	Security is a high skill work environment. Resources must be able to innovate and stay ahead of hackers, and design technology and systems that can beat the continuous evolution of threats. On the other hand adopting advanced network security solutions takes some of the load off of organizations to hire IT professionals.

Source: Frost & Sullivan

Future Trends

Increase in use of mobile devices to launch attacks: Mobile phones and connected devices are likely to be used to breach network security given their propensity to be more vulnerable. As end users use the same devices for business and personal use, end point security becomes critical. According to RSA's 2019 Current State of Cybercrime whitepaper, '70% of fraudulent transactions originated in the mobile channel in 2018'. As the next generation of communication advances with 5G, it also means an increase in the attack surface area for CSPs. The complex and faster networks can expect more malware, security breaches and DDoS attacks.

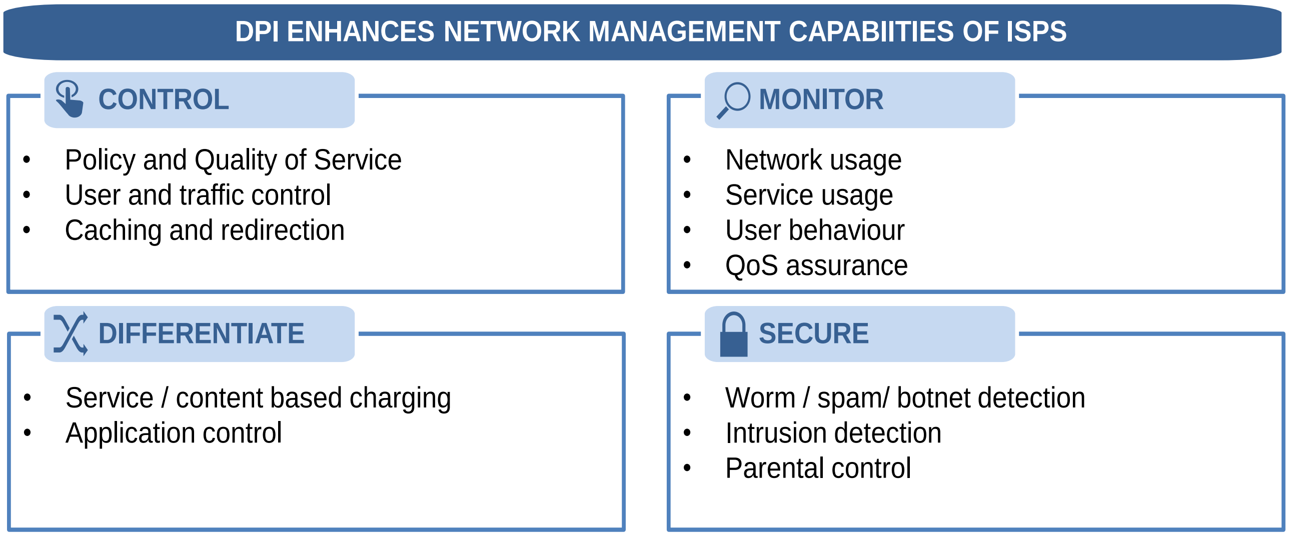
Automation of security systems: Automation creates an added layer of security that is not dependent on human action to secure networks. There is a lack of skilled professionals in the industry, and to enhance their capabilities and utilization, automation can be a critical tool. Most customers lack the requisite expertise and rely on third party providers, another reason for the trend to gain popularity. The growing trend of adoption of AI and ML to power solutions will also contribute. Benefits of these technologies include enabling better response rates, pre-empting threat detection, and insights on effective mechanisms to reduce threats.

Unification and standardization of security orchestration: Network security providers are increasingly looking at ensuring integrated solutions for comprehensive solutions. Haphazard expansion of digital ecosystems can leave systems vulnerable to attacks. Regulations such as GDPR will work towards curbing malpractices and put greater focus on compliance. Since hackers can utilize multiple entry points such as emails, public clouds, etc to enter the system, the need for end-to-end systems to prevent networks with established standards will continue to grow. This should also feed into all network security controls (i.e. physical, virtual, cloud-based) reporting into a common control panel for various activities such as configuration, policy, and change management.

Market Trends: Network Intelligence - Deep Packet Inspection (DPI)

Conventional packet filtering is a basic approach that lacks in sophistication and reads only the header information of each packet with little or no evaluation of the data inside. The low processing power of firewalls makes them incapable of handling large volumes of packets. An alternative is ***Deep packet inspection (DPI)***, which enables network providers to inspect the data being shared in detail at the inspection point. It looks for protocol non-compliance, viruses, spam, and uses defined criteria to decide whether the packet may pass or if it requires rerouting.

DPI helps to maintain the integrity and security of networks by managing and controlling customer usage, speed and type of content, and congestion. The information accrued can also be used for internet data mining, eavesdropping, internet censorship, preventing denial-of-service (DoS) attacks, other sophisticated intrusions, and identifying worms that may fit within a single packet.



DPI ENHANCES NETWORK MANAGEMENT CAPABIITIES OF ISPS

CONTROL

- Policy and Quality of Service
- User and traffic control
- Caching and redirection

MONITOR

- Network usage
- Service usage
- User behaviour
- QoS assurance

DIFFERENTIATE

- Service / content based charging
- Application control

SECURE

- Worm / spam/ botnet detection
- Intrusion detection
- Parental control

Source: Frost & Sullivan, Reports Intellect

Regional Trends

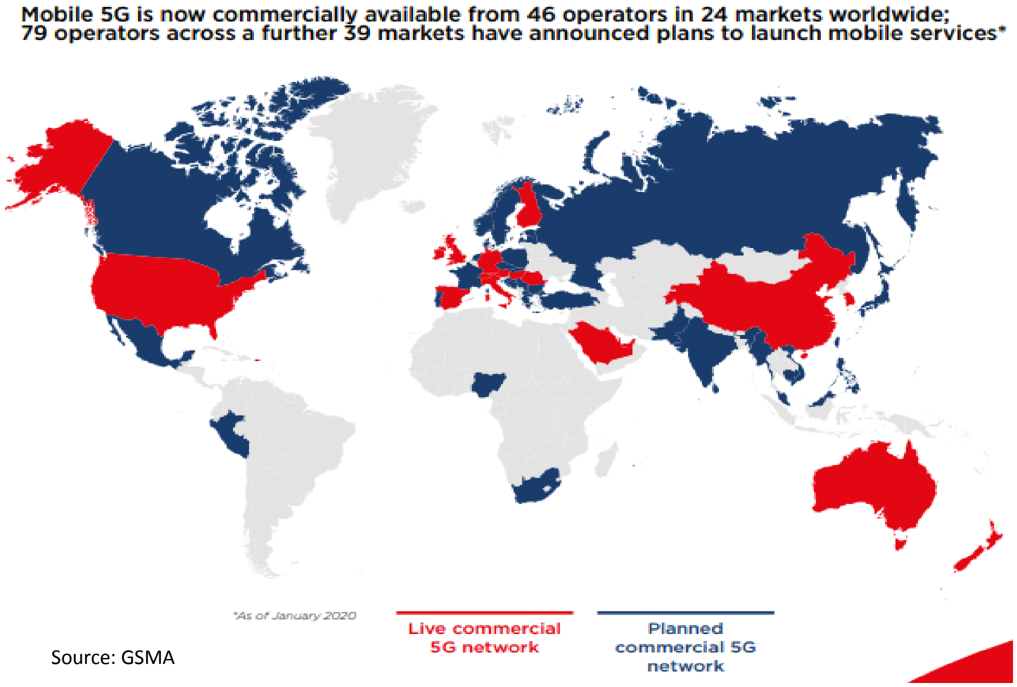
- Europe is the second largest regional market
- It has a number of technologically advanced countries and strict regulations on data.
- The country-specific markets in this region are Germany, France, Spain, Italy, and the UK.

- Asia Pacific is expected to emerge as the fastest rowing market due to high penetration of mobile devices.
- Developed countries are adopting regulations to govern data management.
- Data security however continues to be a concern in other countries.

- NA is the largest regional market, led by the United States and Canada
- The market is driven by :
  - Early adoption and presence of market leaders
  - Strict government regulations on online security of data

Source: Frost & Sullivan

Across the rest of the world (RoW), in regions such as Latin America and Africa, the market is much smaller since the availability and use of advanced technology is limited. We can look to 5G trends in order to extrapolate conclusions on the DPI market because DPI is critical to the success of 5G as mentioned in the executive investment thesis.



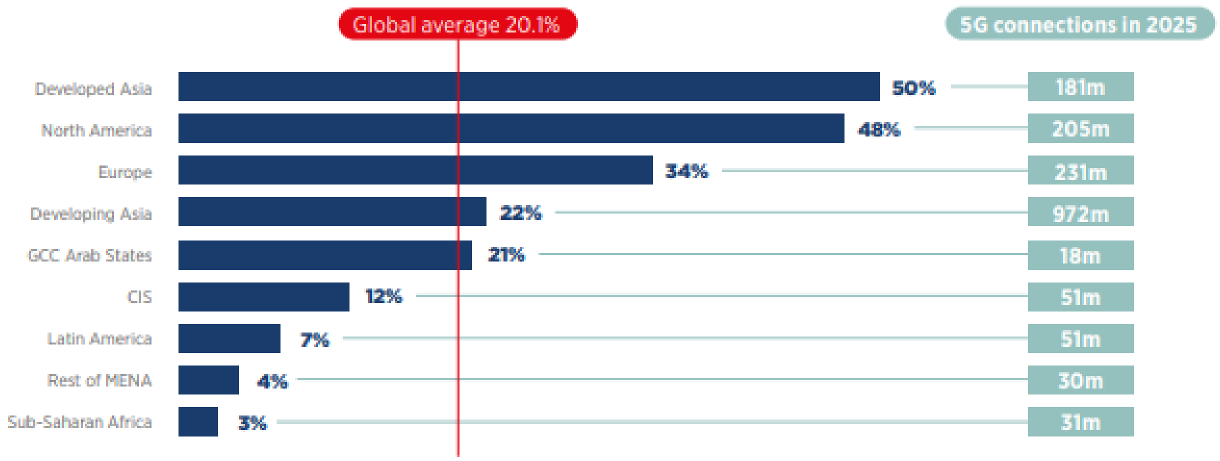
Mobile 5G is now commercially available from 46 operators in 24 markets worldwide; 79 operators across a further 39 markets have announced plans to launch mobile services*

*As of January 2020

Source: GSMA

1.8 billion 5G connections by 2025: developed Asia and the US will lead the way

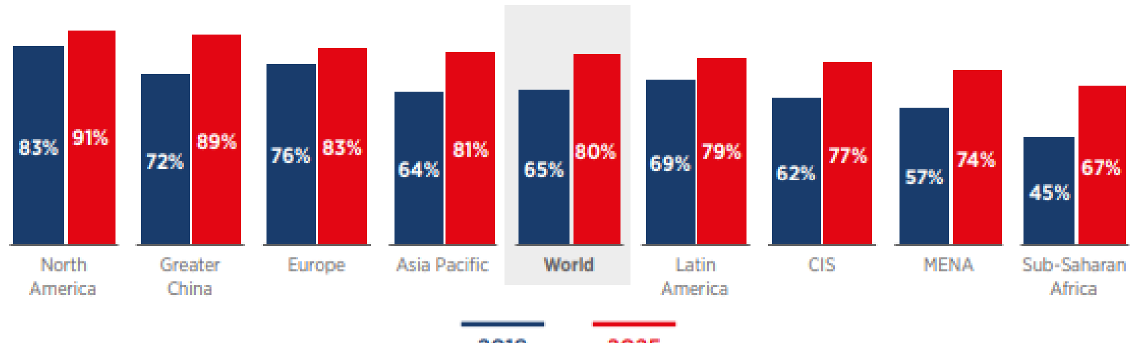
5G adoption in 2025 (% of connections)



Source: GSMA Intelligence

Four in five connections globally will be smartphones by 2025; smartphone connections in Sub-Saharan Africa will nearly double

% of connections (excluding licensed cellular IoT)



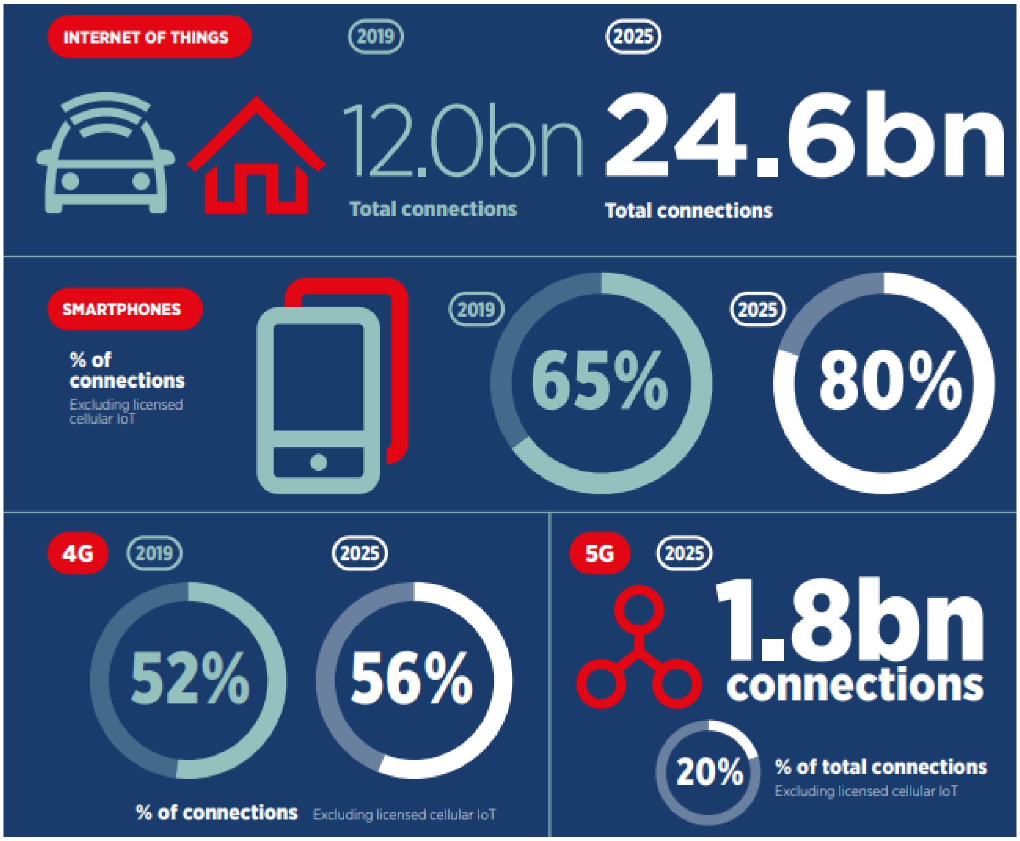
Source: GSMA Intelligence

Trends Impacting the DPI Market

1. **Growing demand for bandwidth-intensive applications** – Global Internet and mobile Internet trends indicate increase in usage of applications that require high bandwidth such as video streaming services. Internet traffic is dominated by video streaming contributing more than 60% of total downstream traffic volume. To deploy network analytics and optimizing strategies, providers will require network and customer insights derived from DPI technology.
2. **Increasing use of tiered service plans** - With the advent of advanced technologies such as Big Data and Analytics (BDA), Machine Learning (ML) and Artificial Intelligence (AI), providers of mobile and broadband services are making attempts to differentiate based on

value-added services and pricing models. Operators tailor offerings based on customer usage to impact average revenue per user (ARPU) for operators. DPI can meet these specific demands by providing specific insights.

3. **Increasing use of connected devices** - The ongoing increase in Internet of Things (IoT) and Machine to Machine (M2M) strategies across verticals means that certain services such as telematics and remote patient monitoring will demand better quality of services (QoS). Users will include DPI as an integral part of the IoT and M2M strategies and providers must offer solutions that are capable of identifying and categorizing traffic generated by connected devices.



Factors Driving Adoption of DPI

The ability of DPI to manage network traffic efficiently is aiding its popularity. Across user groups, its impact on various parameters is driving adoption.

Major Drivers Impacting Adoption of DPI	
Increasing mobile device penetration and 5G	Rising use of mobile devices will also drive demand for mobile broadband data. This will intensify the competition among network providers who will look at an option to enhance performance.
Access to data trends	Access to data trends such as statistical information about usage patterns by different user groups helps to understand user behavior based on their connections.

	The insights reveal trends that can, in turn, enhance network planning.
Need for cyber security	The threat of spam, worms, and viruses is constantly rising. The ‘Internet Security Threat Report’ published by Symantec (U.S.) in 2019, mentions that malware diagnosed in 2018 rose by tens of percent in some sectors.
Enhancing customer experience and engagement to decrease customer churn / Dealing with economies of scale	Due to the growing complexity of network and shrinking operating budgets, operators struggle to meet the QoS and QoE requirements. DPI enables better performance by leveraging automation, analytics and optimizing deployment. Providers have been able to guide their customers to new revenue streams, faster time to market, scaling up and enhancement of end-user experience by optimizing resources.
Innovation possibilities	Documentation and understanding of trends enable innovation at the edge. One such example is online messaging, which replaced expensive international phone calls.

Source: Frost & Sullivan

Factors Constraining Adoption of DPI

The depth of information gained via DPI raises concerns about misuse of insights to influence customer choices and experience, limit options, and at its worst impinge upon the privacy of users.

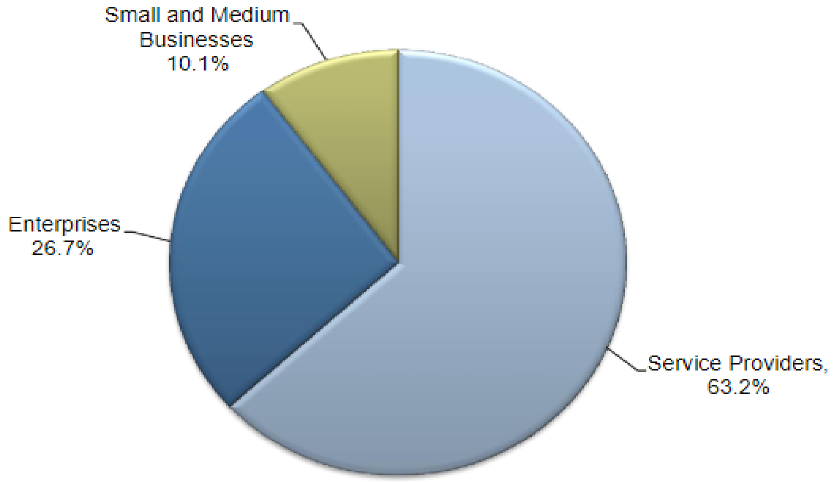
Major Constraints Impacting Adoption of DPI	
Privacy concerns	The content of packets reveals user insights like never before, going into minute details of behavior and enabling inferences about personal interests and purchasing habits. Analysis can be intrusive and be used unfairly by CSPs.
Unethical use of information	DPI appliances can be used to interfere with web-based technologies (such as VoIP) and enable prioritization to benefit commercial agreements. Serious violations may include the introduction of forged packets into the data stream.
Ambiguous regulations	Laws to govern the privacy of data accessed by DPI are ambiguous at best, for instance, in the United States, the secondary use of DPI data is not restricted by law. Users have little control over how the data is used or stored. Companies have been known to utilize the data to conduct experiments on creating strong marketing campaigns.

Source: Frost & Sullivan

We can also look at wireless technology investment to extrapolate insight on customers of DPI technology in the market:

Key Takeaway: Service providers remain the major end-user industry for the wireless technology market.

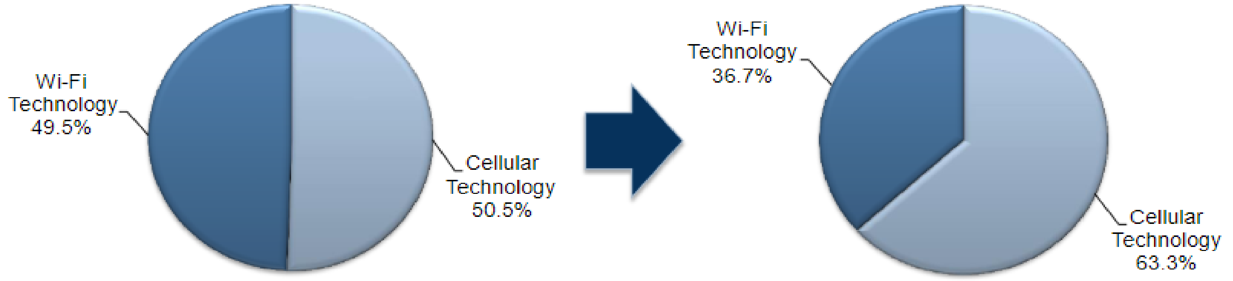
Total Wireless Technology Market: Percent Revenue Breakdown by Industry Vertical, Global, 2019



Key Takeaway: Continuous R&D activities will drive further advancements in cellular communication technology.

Total Wireless Technology Market: Percent Revenue by Segment Type, Global, 2019

Total Wireless Technology Market: Percent Revenue Forecast by Segment Type, Global, 2024



Source: Frost & Sullivan

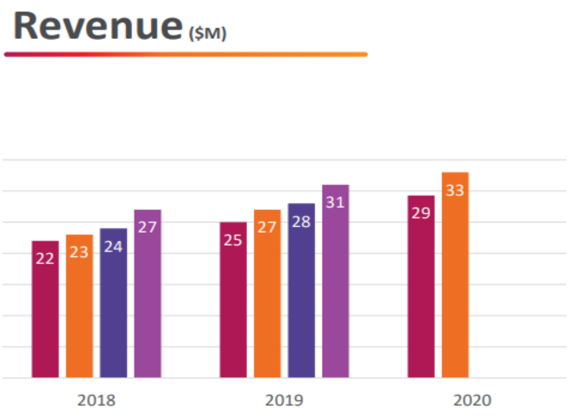
Future Trends

Real-time insights – From communication to video streaming to gaming, the demand for better QoE is only set to increase. Going beyond customization and value addition, use cases such as telematics and gaming require real-time analytics and insights. DPI enabled with analytics and machine learning will impact the level of value addition that operators can provide to end customers.

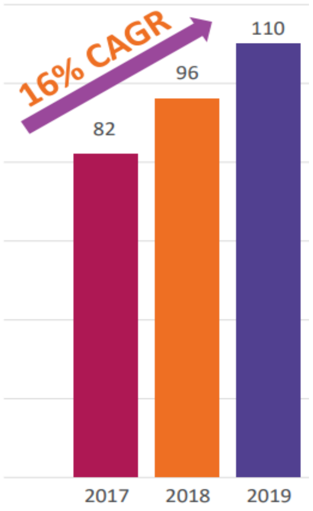
Cybersecurity demand set to grow – The growing sophistication of cyber-attacks need multi-level security. DPI offers an effective tool to companies to tackle cyber-crimes and protect networks and devices from malicious attacks.

Device management - DPI use can be extended beyond mobile core and access networks to devices themselves, enabling operators to better manage traffic signaling, provide mobile security, improve SLAs on enterprise mobility apps and enable more granular subscriber controls such as parental control and shared data plan device control for consumers.

Financial Analysis:



Cash and Investments (30.06.20) $109



Allot generates revenues from two sources: (1) sales of Network Intelligence Solutions which show network operators what is happening on their networks at the highest resolution and (2) sales of Network Security solutions, such as security as a value added service that communication service providers can offer to subscribers in order to protect them from cyber threats. The Company additionally provides maintenance and support services pursuant to a one to three-year maintenance and support program, which may be purchased by customers at the time of product purchase or on a renewal basis.

Exploring the second quarter of 2020 indicates the following:

- Management continues to expect to be profitable in the fourth quarter this year.

- Management continues to expect to close additional Recurring Security Revenue deals in 2020.

- Total revenues for the second quarter of 2020 were $32.8 million, an increase of 23% compared to $26.6 million in the second quarter of 2019.

- Gross profit on a GAAP basis for the second quarter of 2020 was $23.0 million (gross margin of 70.0%), compared with $18.3 million (gross margin of 68.7%) in the second quarter of 2019, representing a 26% improvement.

- Gross profit on a non-GAAP basis for the second quarter of 2020 was $23.2 million (gross margin of 70.7%), a 25% improvement compared with $18.5 million (gross margin of 69.8%) in the second quarter of 2019.

- Net loss on a GAAP basis for the second quarter of 2020 was $3.6 million, or $0.10 per basic share, compared with a net loss of $1.5 million, or $0.04 per basic share, in the second quarter of 2019.

• Non-GAAP net loss for the second quarter of 2020 was $2.4 million, or $0.07 per basic share, compared with a non-GAAP net loss of $2.1 million, or $0.06 per basic share, in the second quarter of 2019.

Net loss includes a $1.5 million doubtful debt expense from a system integrator in Latin America experiencing financial difficulties.

• Cash and investments as of June 30, 2020 totaled $109.2 million, compared with $110.7 million, as of March 31, 2020.

• Since the May 2020 first quarter earnings call, two recurring security revenue expansion deals were signed with existing customers Financial Outlook

• Management reiterates its prior-issued guidance, with expectations for full year 2020 revenues to be between $135 - $140 million, representing accelerated double-digit growth over those of 2019. In addition, management expects that third quarter revenue will exceed those reported for the second quarter of 2020.

Appendix A - Financial Reports

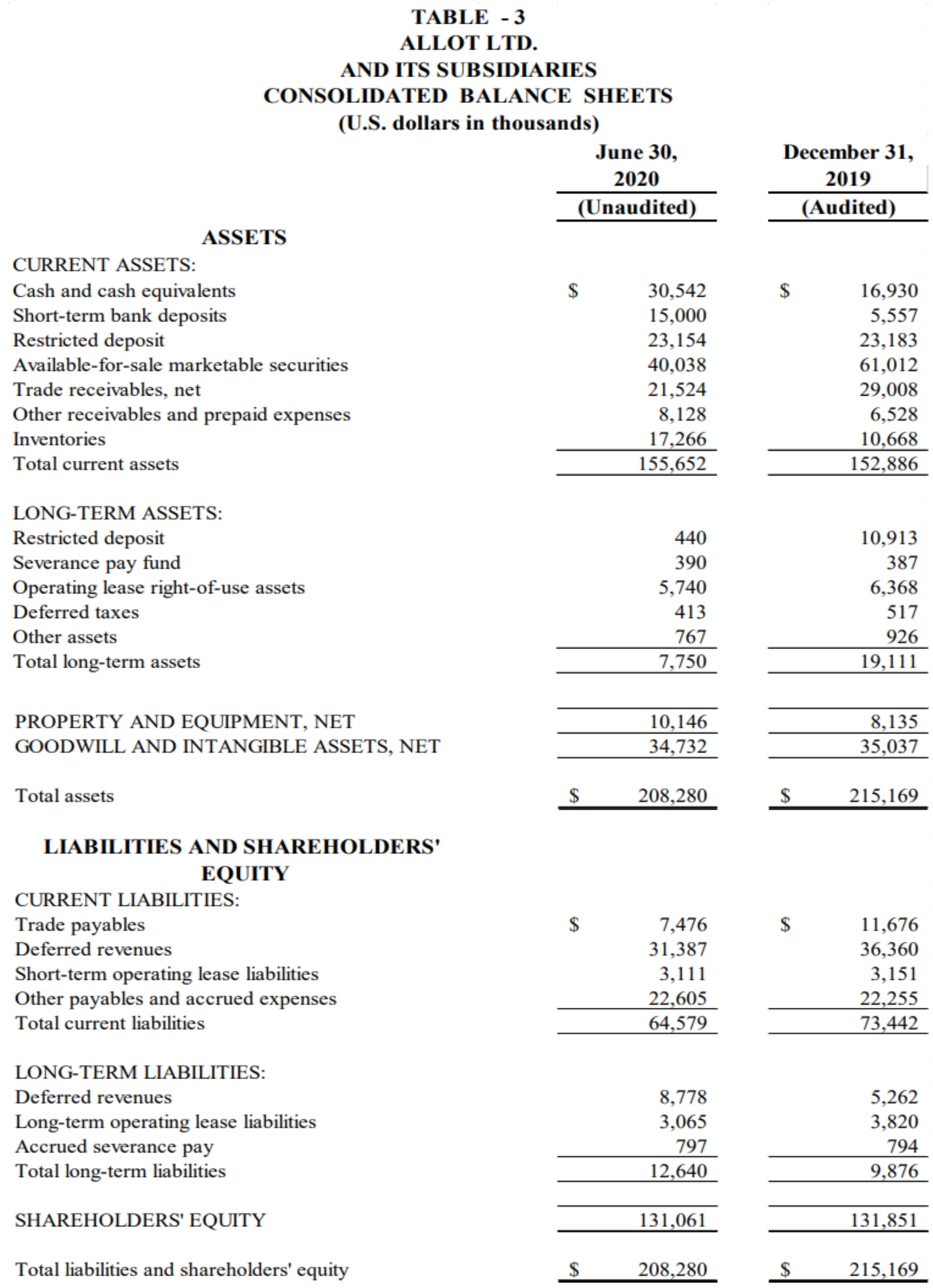


TABLE - 3
ALLOT LTD.
AND ITS SUBSIDIARIES
CONSOLIDATED BALANCE SHEETS
(U.S. dollars in thousands)

	June 30, 2020	December 31, 2019
	(Unaudited)	(Audited)
ASSETS		
CURRENT ASSETS:		
Cash and cash equivalents	$ 30,542	$ 16,930
Short-term bank deposits	15,000	5,557
Restricted deposit	23,154	23,183
Available-for-sale marketable securities	40,038	61,012
Trade receivables, net	21,524	29,008
Other receivables and prepaid expenses	8,128	6,528
Inventories	17,266	10,668
Total current assets	155,652	152,886
LONG-TERM ASSETS:		
Restricted deposit	440	10,913
Severance pay fund	390	387
Operating lease right-of-use assets	5,740	6,368
Deferred taxes	413	517
Other assets	767	926
Total long-term assets	7,750	19,111
PROPERTY AND EQUIPMENT, NET	10,146	8,135
GOODWILL AND INTANGIBLE ASSETS, NET	34,732	35,037
Total assets	$ 208,280	$ 215,169
LIABILITIES AND SHAREHOLDERS' EQUITY		
CURRENT LIABILITIES:		
Trade payables	$ 7,476	$ 11,676
Deferred revenues	31,387	36,360
Short-term operating lease liabilities	3,111	3,151
Other payables and accrued expenses	22,605	22,255
Total current liabilities	64,579	73,442
LONG-TERM LIABILITIES:		
Deferred revenues	8,778	5,262
Long-term operating lease liabilities	3,065	3,820
Accrued severance pay	797	794
Total long-term liabilities	12,640	9,876
SHAREHOLDERS' EQUITY	131,061	131,851
Total liabilities and shareholders' equity	$ 208,280	$ 215,169

TABLE - 1
ALLOT LTD.
AND ITS SUBSIDIARIES
CONSOLIDATED STATEMENTS OF OPERATIONS

(U.S. dollars in thousands, except share and per share data)

	Three Months Ended June 30,		Six Months Ended June 30,	
	2020	2019	2020	2019
	(Unaudited)	(Unaudited)	(Unaudited)	(Unaudited)
Revenues	$ 32,790	$ 26,554	$ 62,079	$ 51,896
Cost of revenues	9,838	8,301	17,448	15,594
Gross profit	22,952	18,253	44,631	36,302
Operating expenses:				
Research and development costs, net	10,396	7,633	19,095	14,807
Sales and marketing	11,780	11,209	23,302	22,686
General and administrative	4,554	923	7,595	3,628
Total operating expenses	26,730	19,765	49,992	41,121
Operating loss	(3,778)	(1,512)	(5,361)	(4,819)
Financial and other income, net	717	571	868	1,103
Loss before income tax expenses	(3,061)	(941)	(4,493)	(3,716)
Tax expenses	553	592	781	1,150
Net Loss	(3,614)	(1,533)	(5,274)	(4,866)

Credit to experts: Chen Yakar

About Frost & Sullivan

Frost & Sullivan* is a leading global consulting, and market & technology research firm that employs staff of 1,800, which includes analysts, experts, and growth strategy consultants at approximately 50 branches across 6 continents, including in Herzliya Pituach, Israel. Frost & Sullivan's equity research utilizes the experience and know-how accumulated over the course of 55 years in medical technologies, life sciences, technology, energy, and other industrial fields, including the publication of tens of thousands of market and technology research reports, economic analyses and valuations. For additional information on Frost & Sullivan's capabilities, visit: www.frost.com. For access to our reports and further information on our Independent Equity Research program visit www.frost.com/equityresearch.

*Frost & Sullivan Research and Consulting Ltd., a wholly owned subsidiary of Frost & Sullivan, is registered and licensed in Israel to practice as an investment adviser.

What is Independent Equity Research?

Nearly all equity research is nowadays performed by stock brokers, investment banks, and other entities which have a financial interest in the stock being analyzed. On the other hand, Independent Equity Research is a boutique service offered by only a few firms worldwide. The aim of such research is to provide an unbiased opinion on the state of the company and potential forthcoming changes, including in their share price. The analysis does not constitute investment advice, and analysts are prohibited from trading any securities being analyzed. Furthermore, a company like Frost & Sullivan conducting Independent Equity Research services is reimbursed by a third party entity and not the company directly. Compensation is received up front to further secure the independence of the coverage.

Analysis Program with the Tel Aviv Stock Exchange (TASE)

Frost & Sullivan is delighted to have been selected to participate in the Analysis Program initiated by the Tel Aviv Stock Exchange Analysis (TASE). Within the framework of the program, Frost & Sullivan produces equity research reports on Technology and Biomed (Healthcare) companies that are listed on the TASE, and disseminates them on exchange message boards and through leading business media channels. Key goals of the program are to enhance global awareness of these companies and to enable more informed investment decisions by investors that are interested in "hot" Israeli Hi-Tech and Healthcare companies. The terms of the program are governed by the agreement that we signed with the TASE and the Israel Securities Authority (ISA) regulations.

For further inquiries, please contact our lead analyst:

Dr. Tiran Rothman **T:** +972 (0) 9 950 2888 **E:** equity.research@frost.com

Disclaimers, disclosures, and insights for more responsible investment decisions

Definitions: "Frost & Sullivan" – A company registered in California, USA with branches and subsidiaries in other regions, including in Israel, and including any other relevant Frost & Sullivan entities, such as Frost & Sullivan Research & Consulting Ltd. ("FSRC"), a wholly owned subsidiary of Frost & Sullivan that is registered in Israel – as applicable. "The Company" or "Participant" – The company that is analyzed in a report and participates in the TASE Scheme; "Report", "Research Note" or "Analysis" – The content, or any part thereof where applicable, contained in a document such as a Research Note and/or any other previous or later document authored by "Frost & Sullivan", regardless if it has been authored in the frame of the "Analysis Program", if included in the database at www.frost.com and regardless of the Analysis format-online, a digital file or hard copy; "Invest", "Investment" or "Investment decision" – Any decision and/or a recommendation to Buy, Hold or Sell any security of The Company. The purpose of the Report is to enable a more informed investment decision. Yet, nothing in a Report shall constitute a recommendation or solicitation to make any Investment Decision, so Frost & Sullivan takes no responsibility and shall not be deemed responsible for any specific decision, including an Investment Decision, and will not be liable for any actual, consequential, or punitive damages directly or indirectly related to The Report. Without derogating from the generality of the above, you shall consider the following clarifications, disclosure recommendations, and disclaimers. The Report does not include any personal or personalized advice as it cannot consider the particular investment criteria, needs, preferences, priorities, limitations, financial situation, risk aversion, and any other particular circumstances and factors that shall impact an investment decision. Nevertheless, according to the Israeli law, this report can serve as a raison d'etre off which an individual/entity may make an investment decision.

Frost & Sullivan makes no warranty nor representation, expressed or implied, as to the completeness and accuracy of the Report at the time of any investment decision, and no liability shall attach thereto, considering the following among other reasons: The Report may not include the most updated and relevant information from all relevant sources, including later Reports, if any, at the time of the investment decision, so any investment decision shall consider these; The Analysis considers data, information and assessments provided by the company and from sources that were published by third parties (however, even reliable sources contain unknown errors from time to time); the methodology focused on major known products, activities and target markets of the Company that may have a significant impact on its performance as per our discretion, but it may ignore other elements; the Company was not allowed to share any insider information; any investment decision must be based on a clear understanding of the technologies, products, business environments, and any other drivers and restraints of the company's performance, regardless if such information is mentioned in the Report or not; an investment decision shall consider any relevant updated information, such as the company's website and reports on Magna; information and assessments contained in the Report are obtained from sources believed by us to be reliable (however, any source may contain unknown errors. All expressions of opinions, forecasts or estimates reflect the judgment at the time of writing, based on the Company's latest financial report, and some additional information (they are subject to change without any notice). You shall consider the entire analysis contained in the Reports. No specific part of a Report, including any summary that is provided for convenience only, shall serve per se as a basis for any investment decision. In case you perceive a contradiction between any parts of the Report, you shall avoid any investment decision before such contradiction is resolved. Frost and Sullivan only produces research that falls under the non-monetary minor benefit group in MiFID II. As we do not seek payment from the asset management community and do not have any execution function, you are able to continue receiving our research under the new MiFiD II regime. This applies to all forms of transmission, including email, website and financial platforms such as Bloomberg and Thomson.

Risks, valuation, and projections: Any stock price or equity value referred to in The Report may fluctuate. Past performance is not indicative of future performance, future returns are not guaranteed, and a loss of original capital may occur. Nothing contained in the Report is or should be relied on as, a promise or representation as to the future. The projected financial information is prepared expressly for use herein and is based upon the stated assumptions and Frost & Sullivan's analysis of information available at the time that this Report was prepared. There is no representation, warranty, or other assurance that any of the projections will be realized. The Report contains forward-looking statements, such as "anticipate", "continue", "estimate", "expect", "may", "will", "project", "should", "believe" and similar expressions. Undue reliance should not be placed on the forward-looking statements because there is no assurance that they will prove to be correct. Since forward-looking statements address future events and conditions, they involve inherent risks and uncertainties. Forward-looking information or statements contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results to be materially different from current projections. Macro level factors that are not directly analyzed in the Report, such as interest rates and exchange rates, any events related to the eco-system, clients, suppliers, competitors, regulators, and others may fluctuate at any time. An investment decision must consider the Risks described in the Report and any other relevant Reports, if any, including the latest financial reports of the company. R&D activities shall be considered as high risk, even if such risks are not specifically discussed in the Report. Any investment decision shall consider the impact of negative and even worst case scenarios. Any relevant forward-looking statements as defined in Section 27A of the Securities Act of 1933 and Section 21E the Securities Exchange Act of 1934 (as amended) are made pursuant to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995.

TASE Analysis Scheme: The Report is authored by Frost & Sullivan Research & Consulting Ltd. within the framework of the Analysis Scheme of the Tel Aviv Stock Exchange ("TASE") regarding the provision of analysis services on companies that participate in the analysis scheme (see details: www.tase.co.il/LPages/TechAnalysis/Tase_Analysis_Site/index.html, www.tase.co.il/LPages/InvestorRelations/english/tase-analysis-program.html), an agreement that the company has signed with TASE ("The Agreement") and the regulation and supervision of the Israel Security Authority (ISA). FSRC and its lead analyst are licensed by the ISA as investment advisors. Accordingly, the following implications and disclosure requirements shall apply. The agreement with the Tel-Aviv Stock Exchange Ltd. regarding participation in the scheme for research analysis of public companies does not and shall not constitute an agreement on the part of the Tel-Aviv Stock Exchange Ltd. or the Israel Securities Authority to the content of the Equity Research Notes or to the recommendations contained therein. As per the Agreement and/or ISA regulations: A summary of the Report shall also be published in Hebrew. In the event of any contradiction, inconsistency, discrepancy, ambiguity or variance between the English Report and the Hebrew summary of said Report, the English version shall prevail. The Report shall include a description of the Participant and its business activities, which shall inter alia relate to matters such as: shareholders; management; products; relevant intellectual property; the business environment in which the Participant operates; the Participant's standing in such an environment including current and forecasted trends; a description of past and current financial positions of the Participant; and a forecast regarding future developments and any other matter which in the professional view of Frost & Sullivan (as defined below) should be addressed in a research Report (of the nature published) and which may affect the decision of a reasonable investor contemplating an investment in the Participant's securities. An equity research abstract shall accompany each Equity Research Report, describing the main points addressed. A thorough analysis and discussion will be included in Reports where the investment case has materially changed. Short update notes, in which the investment case has not materially changed, will include a summary valuation discussion. Subject to the agreement, Frost & Sullivan Research & Consulting Ltd. is entitled to an annual fee to be paid directly by the TASE. Each participant shall pay fees for its participation in the Scheme directly to the TASE. The named lead analyst and analysts responsible for this Report certify that the views expressed in the Report accurately reflect their personal views about the Company and its securities and that no part of their compensation was, is, or will be directly or indirectly related to the specific recommendation or view contained in the Report. Neither said analysts nor Frost & Sullivan trade or directly own any securities in the company. The lead analyst has a limited investment advisor license for analysis only.