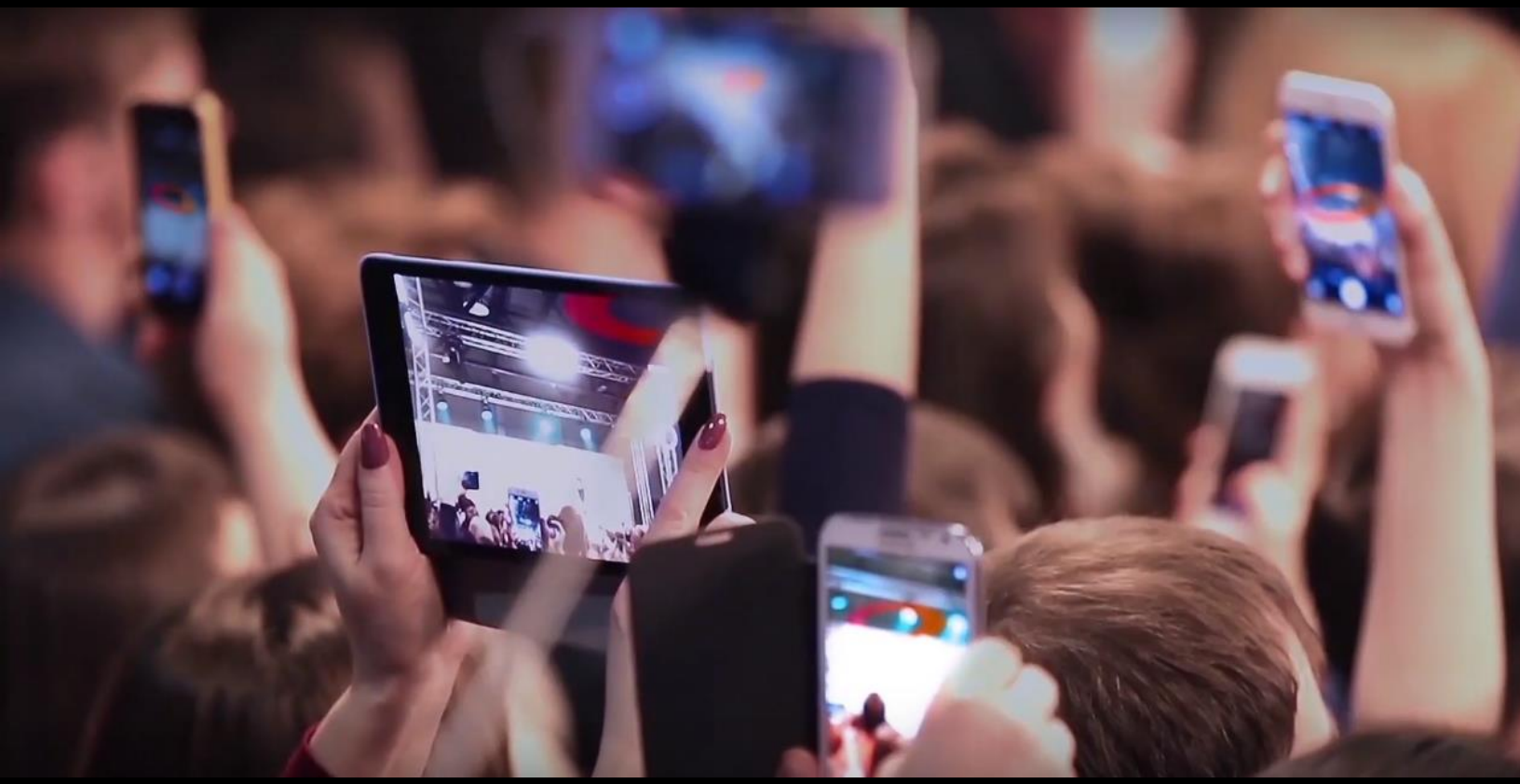
FROST & SULLIVAN

INDEPENDENT EQUITY RESEARCH



allot

FROST & SULLIVAN

Initiation Report October 6, 2019

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 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 Security and Network Intelligence Solutions. These solutions enable entities such as telecom service providers 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 21 million subscribers in Europe.

FROST & SULLIVAN

Allot Allows Telecom Providers to Leverage Their Networks; We view Allot`s Network Security operations as a growth engine for the company's revenues in the coming years; we initiate coverage on Allot at a share price target of 41.8 NIS

Primary Exchange: NASDAQ / TLV

Ticker: ALLT

Sector: Technology

Sub Sector: Software/Internet

Data as at October 6, 2019
(Source: TASE)

Closing price: 27.3 NIS
Market cap: 937.7 million NIS
# of shares: 34.4 million
Stock performance (3 mos.): -1%
Daily-trading-vol. (3 mos.): 62.4k

Stock target price: 41.8 NIS / $12.0

Lead Analyst
Dr. Tiran Rothman

Frost & Sullivan
Research & Consulting Ltd.
A: Abba Even 1, Herzliya Pituach
T: +972 (0) 9 950 2888
E: equity.research@frost.com
W: www.frost.com/equityresearch

Highlights

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 telecom service providers can offer to subscribers in order to protect them from cyber threats. The Company additionally provides support and maintenance services.

In 2018 Allot's non-GAAP revenues amounted to $96 million, an increase from 2017 ($82 million) and from 2016 ($91 million). Total revenues for the second quarter of 2019 were $26.6 million, an increase of 15% compared to $23.0 million in the second quarter of 2018.

Allot has introduced a new management team that is highly experienced and focused on implementing their offering.

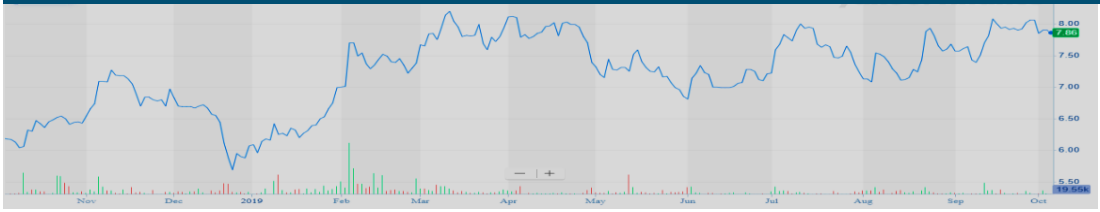
Allot has made a strategic decision to focus its marketing and sales efforts on mobile Network Security reaching out to what seems like the blue ocean of cyber security. **We expect Allot to show a significant increase in revenues over the next 5 years due to the high growth expected in this sector and importantly due to the company's transition from a CAPEX to a Rev-Share business model.**

Allot can be characterized 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 them (one allows customers to see and control their networks and the other to secure them).**

We evaluate Allot's equity value at $411.8 million/1.43 billion NIS; price target is in the range of 41.7 NIS to 42.0 NIS with a mean of 41.8 NIS / $12. Below are our main assumptions and forecast for 2019-2022:

000, $	2018A	2019E	2020E	2021E	2022E
Revenues	95,837	109,037	125,392	158,301	203,553
Gross profit	67,751	77,849	89,271	113,492	145,935
Operating (loss) profit	-4,810	-4,862	-5,059	1,995	12,251

12 Month Price Action (Source: Yahoo Finance)



Executive Summary:

Investment Thesis:

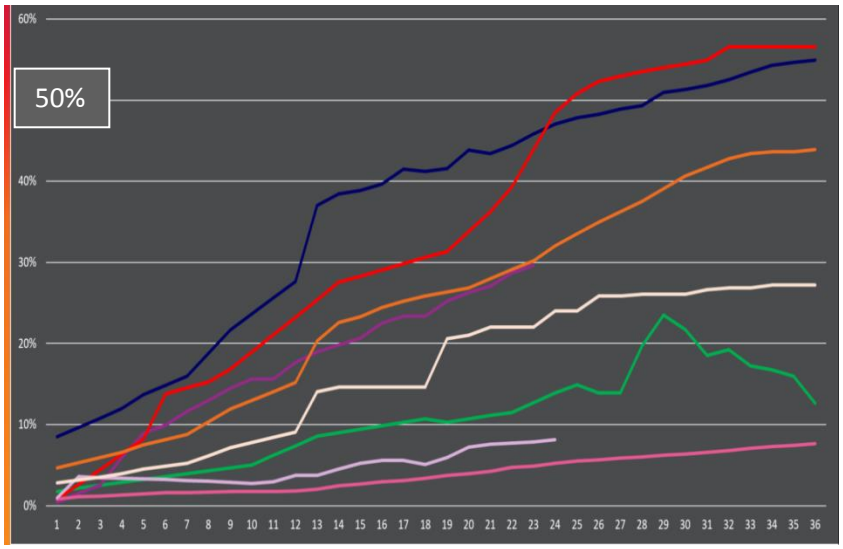
Today's forms of communication have made the world into a very small place. We can easily communicate with our families, friends, and colleagues, on the other side of the world, **via our cellular network,** to message them about the latest episode of our favorite Netflix show, streamed **via our home 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.

The second major problem that arises is that as more and more devices utilize our 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.

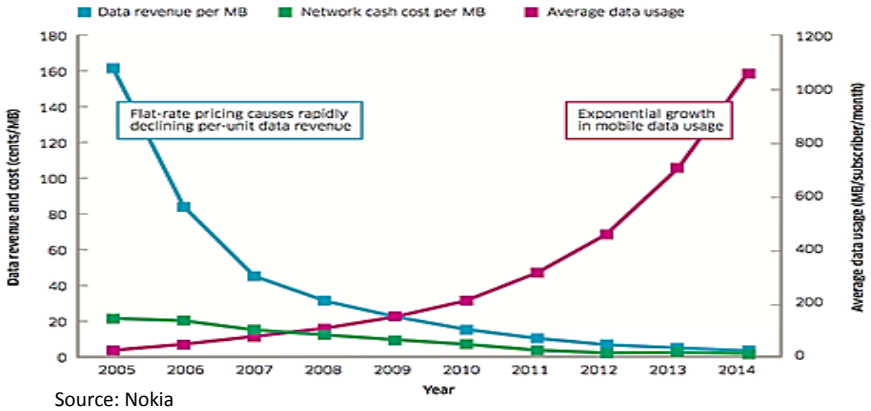
These two developing problems are those that Allot has dedicated itself to solve. The Company's **Network Intelligence** Solution allows CSPs to get more out of their existing network bandwidth so that end users receive high Quality of Experience (QoE) without intensive CAPEX investment. That is, simple broadband pipes, where data flows, become smart and sophisticated allowing CSPs to see what type of data is flowing at high resolution and to adapt to congestion.

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** Solution. 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 network) and not end-point based (they also provide end-point security where necessary) users do not have to download or install anything. They are automatically protected.



The graph to the left shows penetration rates over weeks for different CSPs. We can see that gradually Allot's Network Security solution is achieving penetration rates over 50% for 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: "*Our Secure Net product (provided by Allot) is already 160 million in revenue… we have been building quietly and we will leverage on.*"

The graph below shows that over time mobile data prices have declined exponentially while data usage has increased exponentially. In theory, if data revenue continues to decrease at a rate faster than network costs then revenue per unit of data could become negative. This point is especially important considering that some CSPs are transitioning from tiered services to unlimited data services where they have no control over the revenue per unit of data used.



Source: Nokia

That is why it is critical for CSPs to find ways of reducing their CAPEX investments and to create new revenue streams. Another important trend that is driving adoption of Network Intelligence and Network Security Solutions is the regulatory landscape. Just this year the UK introduced 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. Allot allows CSPs to adapt to the above trends such as the increase in device and data usage, increase in need for security, and increase in need for QoE while limiting CAPEX and creating new revenue streams. Within the competitive landscape Allot is well positioned and provides network awareness and security of the highest quality.

Allot has made a strategic decision to focus its marketing and sales efforts on mobile Network 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. Today Allot has already on-boarded a few Tier 1 telecom customers that offer Allot's security value added service to end users.

The nature of the company can be characterized for 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.

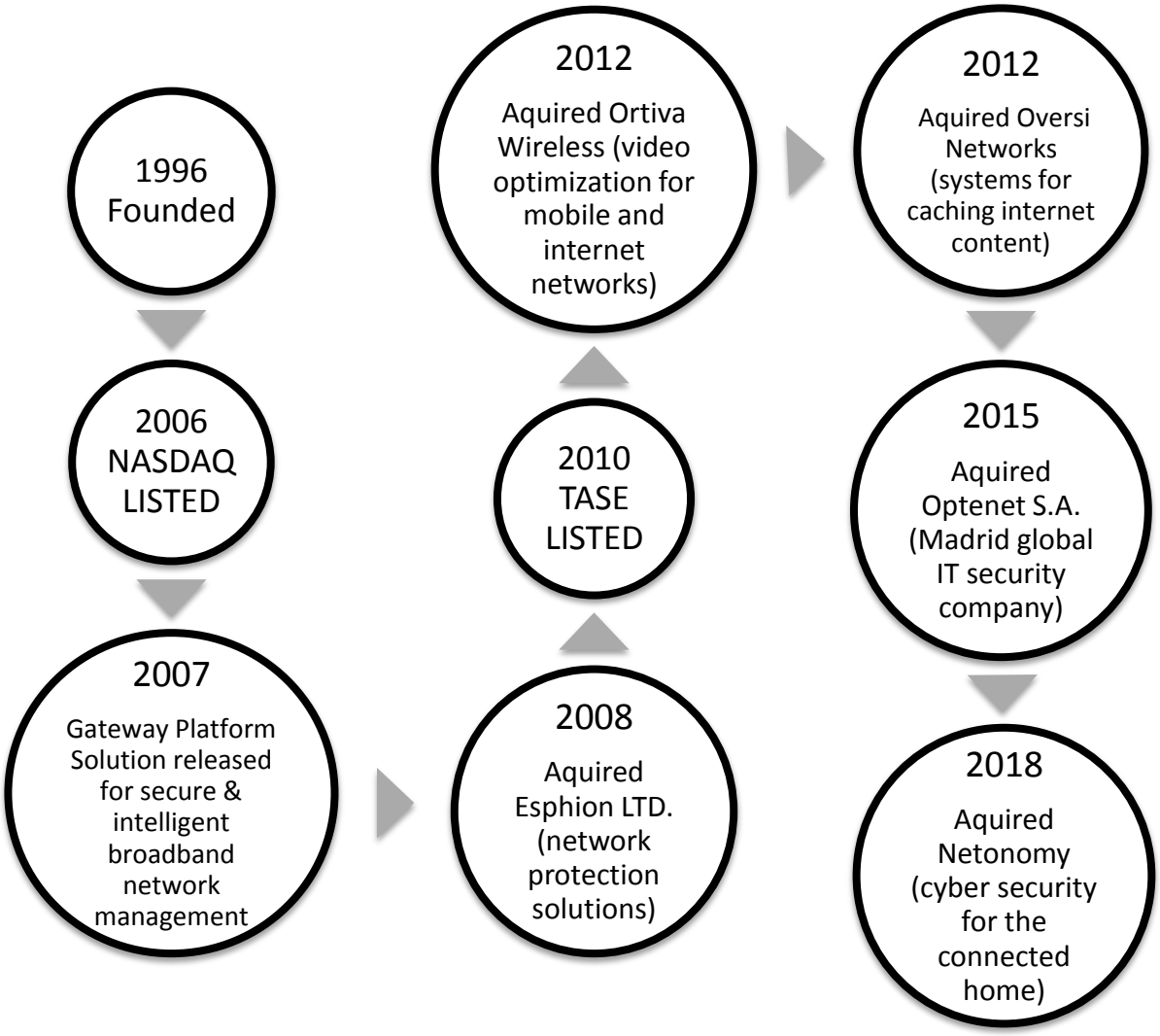
Contents

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.**



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.

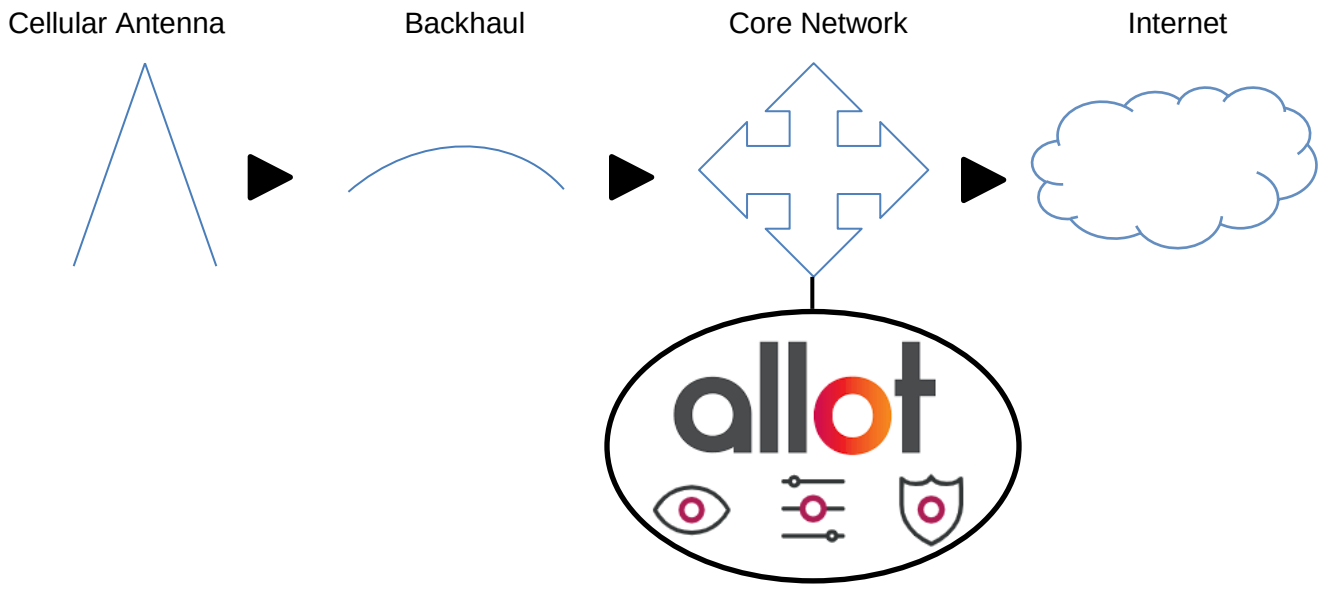
The company's HQ is located in Hod-Hasharon Israel where the principal administrative and research and development activities take place. Additional offices for either sales or research and development are located in the US, Spain, France, Italy, Singapore, South Africa, Columbia, and India.

True to December 31, 2018, Allot has 524 employees of whom 296 are based in Israel, 121 in Europe, 17 in North America, 30 in Latin America, and 60 in Asia, Africa, and Oceania. About 40% of employees engage in R&D, 50% in sales, marketing, and support (Allot puts high emphasis on being customer centric and providing its customers with the support they need), and 10% in management and administration. Allot has introduced a new management team that is highly experienced and focused on implementing their offering.

The breakdown of major shareholders as of Q2 2019 is as follows:

Top current shareholders	Shares	%
Lynrock Lake, L.P.	4,568,039	13.4%
Excellence Investments Ltd.	2,420,949	7.1%
Canaf- Clal Financial Management, LTD	2,157,853	6.3%
Migdal Mutual Funds, LTD	2,015,423	5.9%
Renaissance Technologies, LLC	1,789,725	5.2%
Phoenix Investments and Finance, LTD	1,428,401	4.2%
Fidelity (Canada) Asset Management ULC	1,017,301	3.0%
Harel Insurance Investments and Financial Services, LTD	837,420	2.4%

In order to understand the value proposition of Allot it is important to understand where their solution fits within the big picture. Below is a use-case meant to demonstrate this. The following diagram represents a cellular network:



When you want to watch a YouTube video on your mobile device through your cellular provider your phone makes a request to the nearest cellular antenna. The antenna then sends this request through either physical cables or wireless methods termed “backhaul”. The backhaul carries your request to the core network which is like a highway intersection where data is directed to where it needs to go in the internet to retrieve the YouTube video you want. On the way back from the internet the video is sent back through to the core network to the backhaul to the cellular antenna and to your phone. The YouTube video, sent across the network, is sent in small data chunks termed “packets” because our networks are not designed to send data in one large chunk. Because of this, Network Intelligence Solutions such as Allot‘s are also termed Deep Packet Inspection or DPI solutions. **The core network, where all of the data packets are directed, is where the Allot Network Intelligence and Network Security software sit with a very low signature that does not affect the flow of data. It is at this critical point that Allot’s solution sees, controls, and secures the data packets flowing in the network.**

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 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 intended to protect any and all connected devices from cyber threats. It consists of 5 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), which is a source of added revenue for them.

Allot Smart is powered by deep packet inspection (DPI) technology that supervises and filters the data packets sent over the network. It allows for a cost-effective high quality experience and has the potential to lower access bandwidth costs, defer bandwidth capacity expansions, and reduce revenue leakage. Some of the ways Allot achieves this is by providing visibility and forecasting. 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

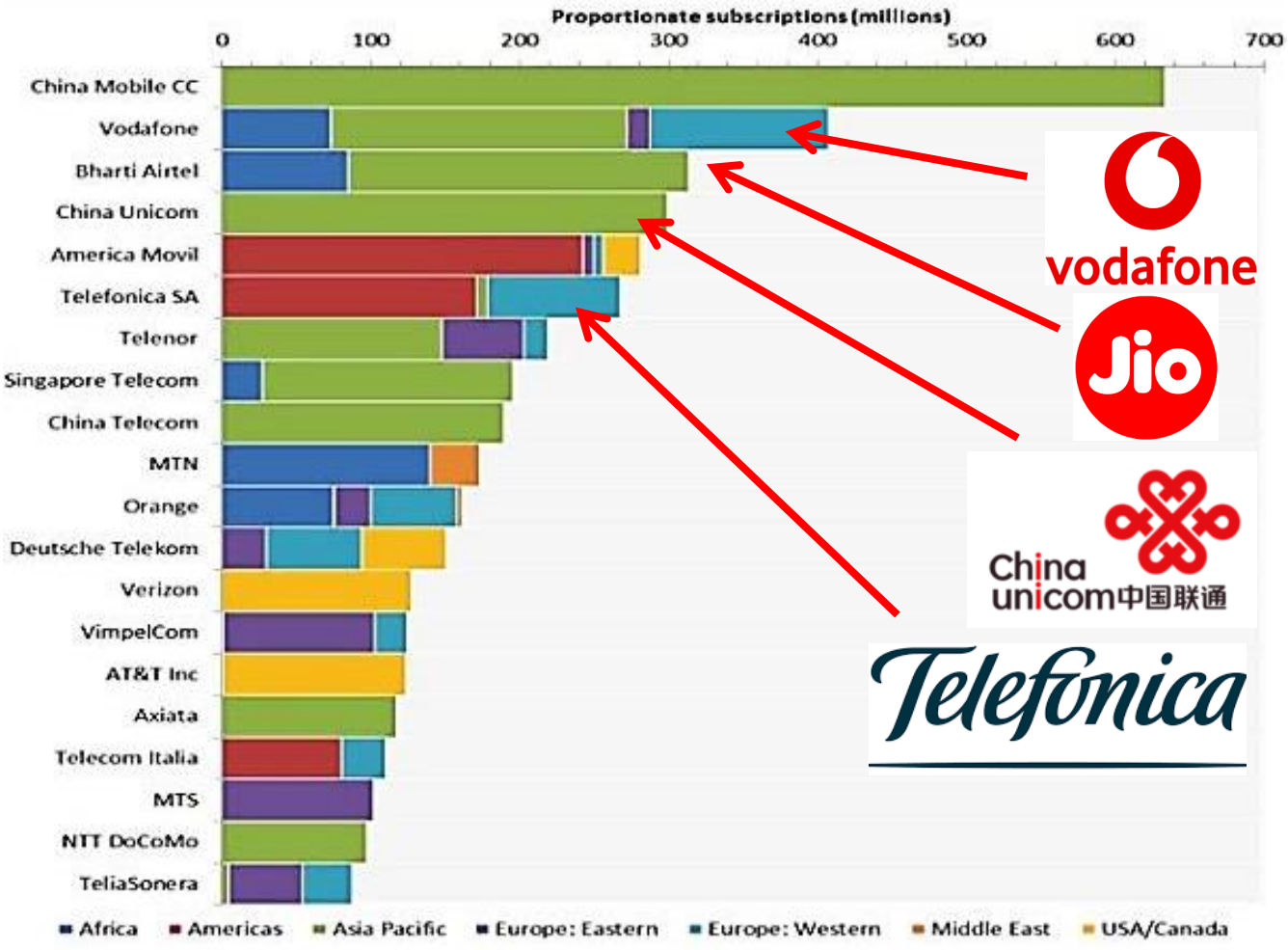
they are able to defer investing in capital intensive network infrastructure for a few years. An additional example would be a CSP having a congested network that does not deliver content at speeds and quality that create user satisfaction. Allot Smart identifies the sources of congestion in a network and mitigates the congestion delivering content that ensures a quality experience (QoE) and therefore limiting churn. For a full list of the significant implications of utilizing Allot Smart including 5G slicing as well as actual use cases implemented for customers see the "Customer" and "Product" section of the report.

Together Allot Secure and Allot Smart are offered under a complete package termed the Allot Secure Service Gateway which is one unified management system that offers the network provider easy to understand analytics on data usage and network traffic, allows for customizable policies, and secures end users against threats. Allot's customers leverage these capabilities to keep customers satisfied, create new revenue streams, and save heavily on CAPEX.

Customers

Allot's 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 has over 1 billion end users. Below you will find a graphic of just some of Allot's customers and 2 case studies clearly demonstrating how customer's implemented Allot's solutions.

Allot provides different services to 13 tier 1 operators. The graphic below shows the largest mobile CSPs in the world by number of subscribers. Four of them toward the top of the list are publically verified Allot customers. For perspective 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.



Source: World Cellular Investors 2015

Case Studies:

❶ 

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 NetworkSecure 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. The Belgian service provider also delivers mobile services, primarily to residential customers in Wallonia and Brussels. VOO has been one of the fastest growing service providers in Europe, currently serving around half a million subscribers.

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

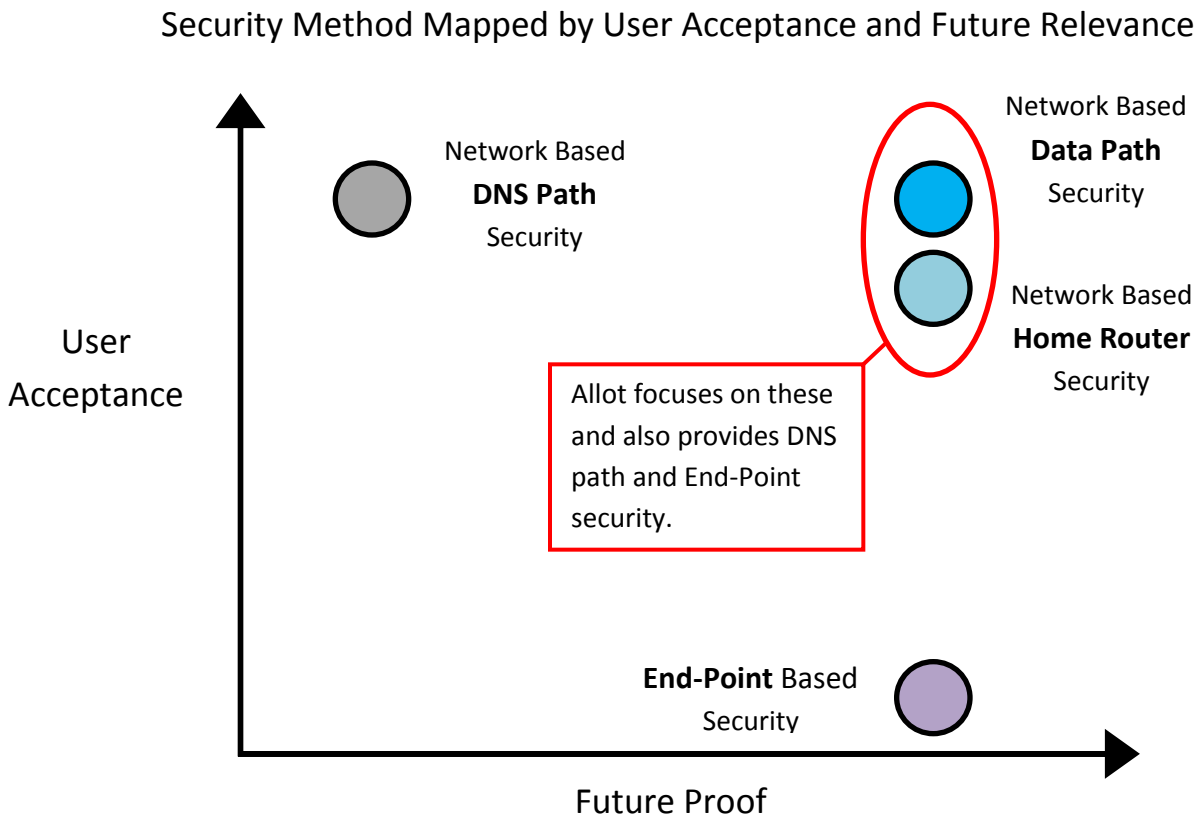
VOO's growth trajectory and ability to attract new customers and keep them, depends on the operator's ability to deliver non-stop access with consistently good quality of service. As a shared media, cable connectivity is highly vulnerable to congestion. VOO's fast expansion was challenged by frequent 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. While frequent network capacity expansion alleviated the congestion temporarily, this was not a sustainable strategy for VOO as the costs involved were very high and the relief was short-lived. They 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. By managing the bandwidth utilization of P2P applications, 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 was activated, VOO saw that their network often sustained 20-40 cyber-attacks per day, with volumes reaching 60 Gbps per attack, and completely saturated network resources. 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:

Competitive Analysis: Network Security



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 Router: security that is present on home 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

phising 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 / Checkpoint / Palo Alto / Secucloud **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 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**	•**Perceived strength**: IoT visibility and protection; per device protection •**Perceived weakness**: slow adoption due to CPE legacy variety; •**Players**: Allot / McAfee / Cujo / SAM / Trend-Micro / F-secure **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.**

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 / F-Secure **Allot works with McAfee and BitDefender to provide End-Point Security**

Competitors

Fortinet: Fortinet's Network Security Solution is an important component of the Fortinet Security Fabric capable of providing visibility and automated threat protection across the entire attack surface using a single operating system to deliver security. Its AI driven solutions help to reduce complexity and provide comprehensive threat protection, in a cost effective way. Network operators benefit from intelligent intent-based segmentation, adaptive access control, and on-premise / multi-cloud threat protection.

With a long history of providing effective solutions, Fortinet is one of the leading providers of comprehensive security solutions. Some of their focus areas are firewalls, anti-virus, intrusion detection and protection, advanced threat protection, secure unified access, and endpoint security. Fortinet utilizes Security Processors (SPUs), a security-focused operating system, and applied threat intelligence to enhance security and visibility for customers. Its partnership strategy enables it to expand its offerings further to meet the challenges that come with expanding attack surfaces.

Palo Alto Networks: is a multinational cybersecurity company that offers a platform with advanced firewalls and cloud-based security products to extend those firewalls to cover other aspects of security. With 60,000 customers across ~150 countries, its products are used by ~85 of the Fortune 100 companies and 63% of the Global 2000. The company's core Security Operating Platform utilizes analytics to automate routine tasks, and simplify security. The Platform automates threat identification and enforcement across the cloud, network and endpoints, blocks ransomware, malware and

fileless attacks. It works across a range of verticals. Other products include cloud security, advanced firewall, endpoint protection and threat detection and prevention.

One of its flagship products, Cortex uses AI. It is an open and integrated AI-based continuous security platform, and AI helps it to constantly evolve to stop sophisticated threats. As part of its growth plans to meet changing requirements of customers the company recently announced its intent to acquire a definitive agreement to acquire Zingbox, an IoT security company. Zingbox offers a cloud-based service and advanced AI and ML technology to identify threats from devices and is likely to enable Palo Alto Networks to enhance IoT security through its Next-Generation Firewall and Cortex™ platforms.

McAfee: One of the well-known cybersecurity companies, McAfee has a long history of providing cybersecurity software. It was acquired by Intel in 2011 as part of its security division. The company has a large corporate and government client base across the globe using products such as McAfee Global Threat Intelligence to help thwart hackers. McAfee's endpoint and mobile security products protect end-user devices from attacks. Its network security capabilities protect company servers, databases and data centers. McAfee provides security software to protect mobile devices and personal computers for home users.

McAfee uses a range of growth strategies. The company recently announced the acquisition of NanoSec, a multi-cloud, zero-trust application and security platform. The acquisition is expected to help application delivery speed, enhance governance, compliance and security of customers' hybrid, multi-cloud deployments. Other efforts include McAfee Security Innovation Alliance (SIA) and McAfee CASB Connect Program, which was recently expanded with the addition of 13 new partners, and six newly certified integrations. McAfee also has a research lab to incorporate advancements in technology in its solutions. The company also partners with network providers to enable better security for consumers. For instance, McAfee's Safe Family enables parents to monitor and control children's online activities.

F-secure: The Company offers security solutions for enterprises and homes. Its global intelligence network, software and AI based solutions focus on prevention, detection and response as a service. F-secure has identified managed endpoint security as a strong growth area. The products are designed to be delivered from the cloud. Its solutions include digital Safety solutions for consumers to protect information, identities, devices, smart homes and families.

The company relies on a partner ecosystem to expand its reach in the market. With a focus on helping customers develop a holistic approach to cybersecurity, the company recently launched the Global Partner Program to connect B2B IT resellers with F-Secure. This will enable them to offer cybersecurity expertise and services to customers using a tiered structure depending on IT reseller capabilities. F-Secure currently partners with more than 200 communication service providers globally. It recently joined the Broadband Forum to help with development of industry standards for the connected home and secure home broadband experience. The company recently acquired MWR InfoSecurity to strengthen its cyber consulting and managed security services such as phishing protection and cyber-attack detection.

Akamai: Akamai uses a multi-layered approach to network security and enables customers to supplement perimeter defense with cloud security. Upon acquisition of Nominum in 2017, a DNS-based security solutions provider, Akamai was able to offer this solution to enterprises. Akamai Intelligent Platform™ offers a portfolio of cloud security solutions that stops attacks at the edges of the Internet. Some of its solutions include Enterprise Application Access meant to secure access, centralize access control and reduce breaches; Enterprise Threat Protector that proactively protects against

malware at the DNS layer; Prolexic Solutions that mitigates DDoS attacks; and the Web Application Firewall to detect potential attacks in HTTP and SSL traffic upstream.

The company has in recent years focused on the enterprise cloud security market. As part of its growth and portfolio development strategy it acquired companies like Prolexic Solutions (Security solution for DDoS attacks at the network, transport, and application layers) and Bloxx (Cloud security provider). The company is continuously adding to its platform capabilities to create stronger solutions. For instance it recently launched Edge Cloud, to leverage the Akamai edge platform to streamline and secure data delivery to connected devices and in-application messaging at scale. Edge Cloud is designed to serve the needs of businesses bringing billions of endpoints online as part of the IoT connected device revolution and further boost the adoption and power of in-application messaging. Companies with multi-cloud strategies rely on Akamai's intelligent platform and its portfolio of edge security, web and mobile performance, enterprise access and video delivery solutions.

Infoblox: Infoblox is a provider of Secure Cloud-Managed Network Services and offers network security as part of its solutions. As part of its 'Next Level Security' approach, the company enables clarity and consolidated single view for the core network. This helps to identify attack points, unmanaged and vulnerable devices; enhances automatic detection and DNS attacks. The 3rd party integration has further enabled an ecosystem that is able to improve infrastructure security and threat intelligence. Detailed reports and insights enhance security teams' capabilities to plan, execute and respond to security issues.

Infoblox recently launched a security platform, BloxOne™ Threat Defense, a hybrid security that can leverage DNS as the first line of defense to detect and block sophisticated cyber threats. As part of its efforts to create an ecosystem to offer comprehensive solutions to customers, Infoblox focuses on a partner sales strategy. It expanded its partner alliance ecosystem by adding 100 new partners in 2018 and continues to focus on further expansion in 2019.

Kaspersky: Kaspersky has a comprehensive suite of security solutions and a long history of providing security solutions to consumers and enterprises. A global cybersecurity provider, its capabilities to offer security solutions extend across small and large corporates, infrastructure and consumers. It has more than 400 million users and 270,000 corporate clients. Some of its security products for consumers include anti-virus, Internet security, Security Cloud, etc, while products for enterprises include Endpoint Security, Hybrid Cloud, and IoT and embedded, among others.

The company is committed to continuous innovation, a fact corroborated by Kaspersky Enterprise Blockchain Security that helps in assessing applications working on a blockchain infrastructure and conducts an audit of smart contract code. Over the years the company has been working closely with organizations such as Interpol to identify cyber threats.

Symantec: Symantec has a long history of providing security solutions and is present in more than 35 countries. With $4.8 billion in revenue for the fiscal year 2017, it has over the years accumulated more than 2,000 global patents. The company offers solutions to enterprises and individuals with integrated solutions to help them stay secure against sophisticated attacks across endpoints, cloud and infrastructure. Symantec's Integrated Cyber Defense (ICD) Platform combines many parameters to offer information protection, threat protection, identity management, compliance and other advanced services to its customers. The Platform is driven by shared intelligence and automation across endpoints, networks, applications, and clouds. With AI, ML, APIs the platform can offer future proof solutions for its customers.

Symantec recently announced a new cloud access security solution as part of its ICD Platform, for enterprises that can secure cloud and internet access and use. This integrated cloud-delivered solution helps companies to lower operational costs and complexity, and risk. More than 120 companies have joined Symantec in its efforts to further reduce the cost and complexity to ensure cyber security and improve response times. Some of the partners are AWS, Box, IBM Security, Microsoft, Oracle, ServiceNow, Splunk, and technology innovators that the company collaborates and integrates with its ICD Platform.

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 bypassing 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 three types of players: 1) **Pure players**, which include only Allot and Sandvine, 2) **DPI library providers** which include players such as Qosmos, and 3) **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).

DPI library providers offer a solution that needs to be integrated with another solution that takes the DPI network visibility component and adds a control component to it so that the insights gathered from the network can be acted upon.

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.

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) Allots 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

Competitors

Sandvine: Sandvine and Procera merged in 2017 to create a strong competitor 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 enhanced and the combined company would be able to target growth opportunities of 5th generation wireless networks, Internet of Things (IoT), software-defined networks and network function virtualization. The joint client portfolio expanded to more than 200 Tier 1 service providers covering > 1.7 billion subscribers, > 500 enterprise customers, and > 40 OEM partners across ~100 countries.

The merger was also likely to accelerate product innovation in Behavioral Analysis, Automation, and Cloud solutions; expanded breadth of use case capabilities such as Network Intelligence market for Analytics, Policy and Charging Control, Security, Regulatory Compliance, Traffic Management, and Cloud Managed Services.

Qosmos: The Qosmos DPI business unit of ENEA provides DPI-based IP traffic classification & network intelligence technology used in physical, SDN and NFV architectures. The software enables real-time application visibility in their

products for traffic optimization, service chaining, quality of service, analytics, cybersecurity and more. ENEA's Qosmos customers benefit from fast time to market and continuous signature updates for their products. The company provides solutions to more than 90 telecom, networking and security vendors worldwide.

The company has launched new functionalities and enhancements to its products and garnered new business in the last 18 months. Some of these are:

- Signed an agreement worth $2.8m for embedded DPI technology for a US-based market leader in cloud technology and SD-WAN solutions for enterprises.
- ENEA's Qosmos ixEngine that delivers real-time traffic visibility to networking and security products by identifying protocols and applications in network packets was further enhanced to include LAN Device Identification, First-Packet Classification, a Traffic Detection Module and categorization of unclassified traffic. The granular traffic visibility helps to optimize traffic, manage data flows, improve service quality and identify security breaches.
- In 2018, Qosmos Probe 2.0 configured as a Deep Packet Inspection (DPI) sensor, was launched. It is designed to strengthen cyber threat hunting capabilities at Security Operations Centers (SOCs).

Arbor Networks (Netscout): Arbor Networks is the security division of Netscout. It offers DDoS protection and network visibility solutions for visibility and traffic intelligence. Arbor's Active Threat Level Analysis System (ATLAS) is a comprehensive solution that provides an overview of internet traffic, trends and threats. It also enables actionable and situational intelligence about botnets, DDoS attacks and malware. The company's DPI solution can analyze service performance issues, evaluate service degradations, enhance user experience by reducing impact of mean-time-to-repair (MTTR) issues, integrate DPI capability into a single management platform to increase efficiency and reduces operational costs and complexity.

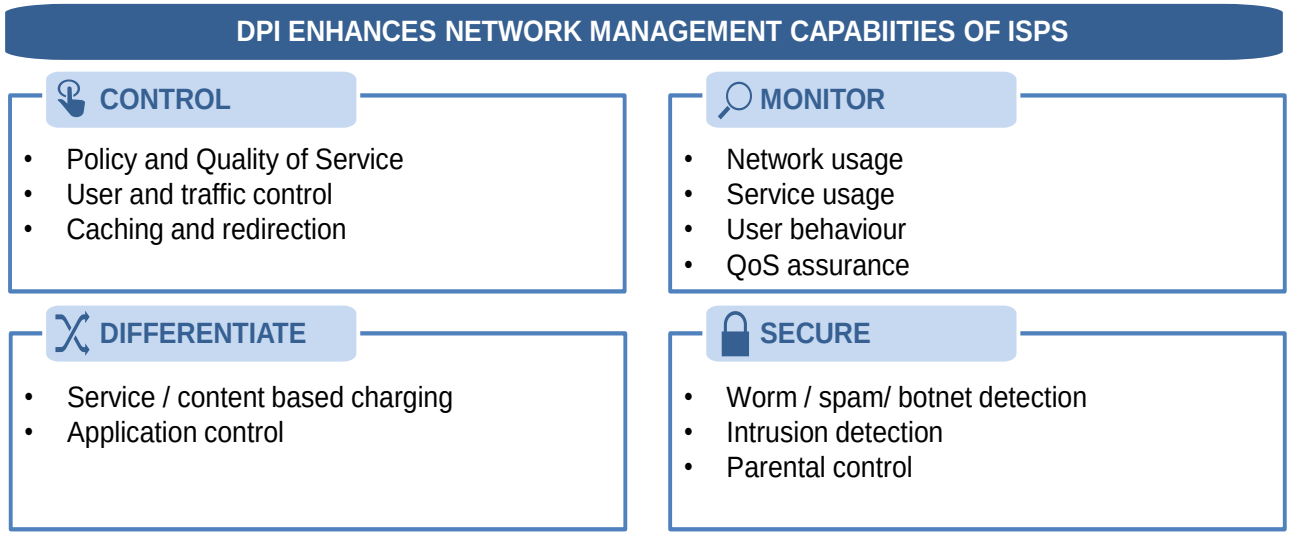
The company recently launched Arbor Threat Analytics (ATA), a network-based threat detection and analytics platform to provide full visibility into multi-cloud environments and enable faster threat detection. This enables NETSCOUT to offer comprehensive threat intelligence by integrating the new solution with its proprietary ATLAS Intelligence Feed that uses ML.

Market Overview

Market: 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. 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.



Source: Frost & Sullivan, Reports Intellect

There are a number of ways to segment the market. In the “Competition” section use product-based segmentation.

Market Segmentation of DPI	
Application-based	• Data loss/leak prevention and management • Network performance management
Product-based	• Standalone DPI • Integrated DPI
End user based	• Internet service providers (ISPs) • Enterprises.

Source: Frost & Sullivan

The capabilities of DPI can be utilized by different user groups for various purposes, based on the intended outcome. The high adoption of Internet and connected devices that link to enterprise systems mandate a more comprehensive security tool to protect against any unauthorized access. Using firewalls alone may not be the most sophisticated and effective technique. Using DPI can enable IT administrators and security officials to set and enforce policies across all layers to ward off threats. For instance, DPI can facilitate data leak prevention (DLP) by guiding a user with information on obtaining clearance to send a confidential file via email.

Frost & Sullivan contend that the DPI market is expected to grow from about $7 Billion in 2016 to $17 Billion in 2021 at a CAGR of around 20%.

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. However potential markets such as Argentina and Brazil higher awareness and can be expected to drive demand.

Trends Impacting 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. According to Sandvine's 2019 Global Internet Phenomena report, 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	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	Quality of experience (QoE) is a key metric driving DPI adoption. It helps to increase efficiency across subscriber management, bandwidth management for P2P applications, and security requirements for enterprise customers. Ensuring QoE decreases customer churn.
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	
Net neutrality laws	Inspection of the content layers is considered against principles of open access of the Internet and something that undermines infrastructure of the internet.
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 ISPs.
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

Challenges / Insights

Calls to curb DPI — DPI is considered to be an effective tool to ensure high-quality service and rational allocation of limited bandwidth. Academics, public service organizations and privacy advocates are increasingly calling for anti-DPI regulations. Net neutrality is expected to be significantly impacted as regulations to monitor how the data is used by different user groups are insubstantial.

Driving 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.

Use Cases

Among the use cases where DPI is specifically used:

- Service/ content based charging
- Policy enforcement such as parental controls
- Quality of Experience (QoE) Assurance
- Quality of Service (QoS) Assurance
- Network congestion mitigation
- 5g slicing
- Network managers can ease the flow of network traffic enabling high priority messages or mission-critical messages to pass through before others.
- Customization of data usage by mobile service operators and prevention of illegal downloading of content

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.

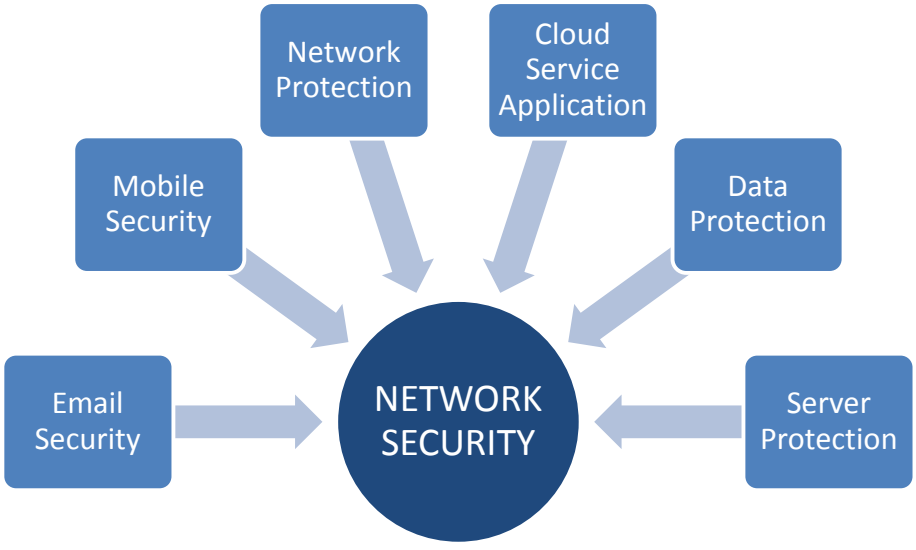
Market: Network Security

The developments in communication and associated technologies have undergone a significant change. 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. Network security uses different practices such as active and passive deployment of software that can track, and stop malicious activities; preventive deployment to identify potential threats and security glitches; and ensures that users are aware of and following security protocols.

Network security providers are capable of a comprehensive assessment of network architecture and evaluation of the security of Internet and Intranet connections. A customized security solution based on users' systems comprising different components such as firewalls can be provided. Additionally, monitoring and end-to-end visibility enable better network security management. After a thorough vulnerability assessment, network security is deployed along with threat intelligence, endpoint security, application security, and other cybersecurity services.

The primary areas of application of network security are detailed in the graphic below:



Source: Frost & Sullivan, Talari Networks

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). The areas where network security may be provided as a service to subscribers are covered below and are compared in the "Competition" section of the report.

Network Security Market
Network based - Data Path
• Security that is located in the network itself and not on our devices **(users do not need to download anything and are automatically protected at no battery cost to devices).**
Network based - DNS Path
• Security that keeps users away from known malicious websites**.**
Network based - Home router
• Security **that is present on home routers.**
End-point based – Applications
• Security that is downloaded on our devices.

Trends Impacting 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. This mandates visibility and mapping of secure access to data and resources based on user and location. It helps to reduce pathways for attackers and malware. It also requires inspection and logging all traffic, implementing security rules based on business policies and using multiple authentication methods to counter attacks.
2. **Enterprise mobility changes the requirements**—Emergence of the BYOD trend is directly related to an increase in enterprise mobility as companies adjust to employees' preferences for smartphones, tablets, and portable computers at work. 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.

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	
Digital 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

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

Challenges / Insights

Different approaches to security—Network complexity increases manifold as a host of different industry participants and third parties come together to help a network function. Importance of network security will be at different levels of priority and not all third party providers will invest equally. Their approach may leave some weak spots in network security.

Breaches go undetected—In spite of implementing network security, it is important to constantly monitor networks since breaches can go undetected for months. To prevent this, efforts to monitor across multiple layers are made to enable comprehensive monitoring and control.

Development of Comprehensive Ecosystem—Over the last few years network security has moved beyond piece-meal implementation to creating end-to-end solutions. As ISPs offer this as a value added service to customers, the solution becomes a critical entity in ensuring protection not just for end users but for ISPs themselves. To ensure this, multiple

innovative companies – large firms, start-ups and technology enablers are working together to enhance and create effective solutions. Increasingly platforms that can integrate different components from different providers are becoming go-to solutions.

Use cases

Some of the use cases where Network Security is used:

- For end-to-end network traffic inspection: Network security has moved beyond perimeter security to include communication in the cloud, and network communications from remote locations to software as a service (SaaS) applications.
- Work across encrypted/decrypted solutions: While most data is encrypted, the network security can detect suspicious traffic without the need to decrypt each time.
- Secure access with network security solutions ensure only trusted users such as end-user devices, APIs, IoT, micro-services, and containers, gain access. It prevents gaps in visibility. Better visibility enhances threat detection, highly secure access, and software-defined segmentation.
- Providing protection from ransomware and to prevent entry from the DNS layer to email to the endpoint.

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 ISPs. 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.

Company's Products:

Allot's products fall under 2 main categories.

1) **Security Solutions:** These secure our connected devices against threats.
2) **Network Intelligence Solutions:** These allow for the optimization of the communication networks that deliver content to our connected devices.

Regardless of the specific product, Allot has 3 motifs that characterize each of its products. Firstly, **they easily integrate with existing customer infrastructure**. Second, **they give well communicated feedback** about what is happening on customer networks. Lastly, **they maximize revenue generating opportunities for customers**.

Their solutions achieve the following for network operators:

- Clear understanding of what is happening in their network through granular analytics.
- Assure optimal network performance, utilization, and customer QoE via traffic control and shaping.
- Drive increased revenue and customer satisfaction through network-based security services.
- Comply with government regulations for safe internet activity.
- Protect local, national and enterprise networks against threats such as volumetric DDoS attacks.
- Reduce OPEX and CAPEX via methods such as forecasting, closed loop automation, and fully NFV compliant deployments.

Allot's products are network agnostic and can be incorporated into any type of network that supports our connected devices including mobile, fixed, satellite, and cloud networks. Their solution turns simple broadband pipes into smart and sophisticated ones allowing for 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. Their solution is network-based (it is located on the network and not on our devices), so it is accessible to any device, does not require end user software or installation, and does not impact performance or battery life.

Allot's solutions can be incorporated via hardware supplied by Allot themselves or via their customer's existing hardware. Their solution is also fully NFV compliant. This means that it can integrate into any network regardless of how it is structured.

The two main platforms by which they offer their services are **Allot Secure** and **Allot Smart**.

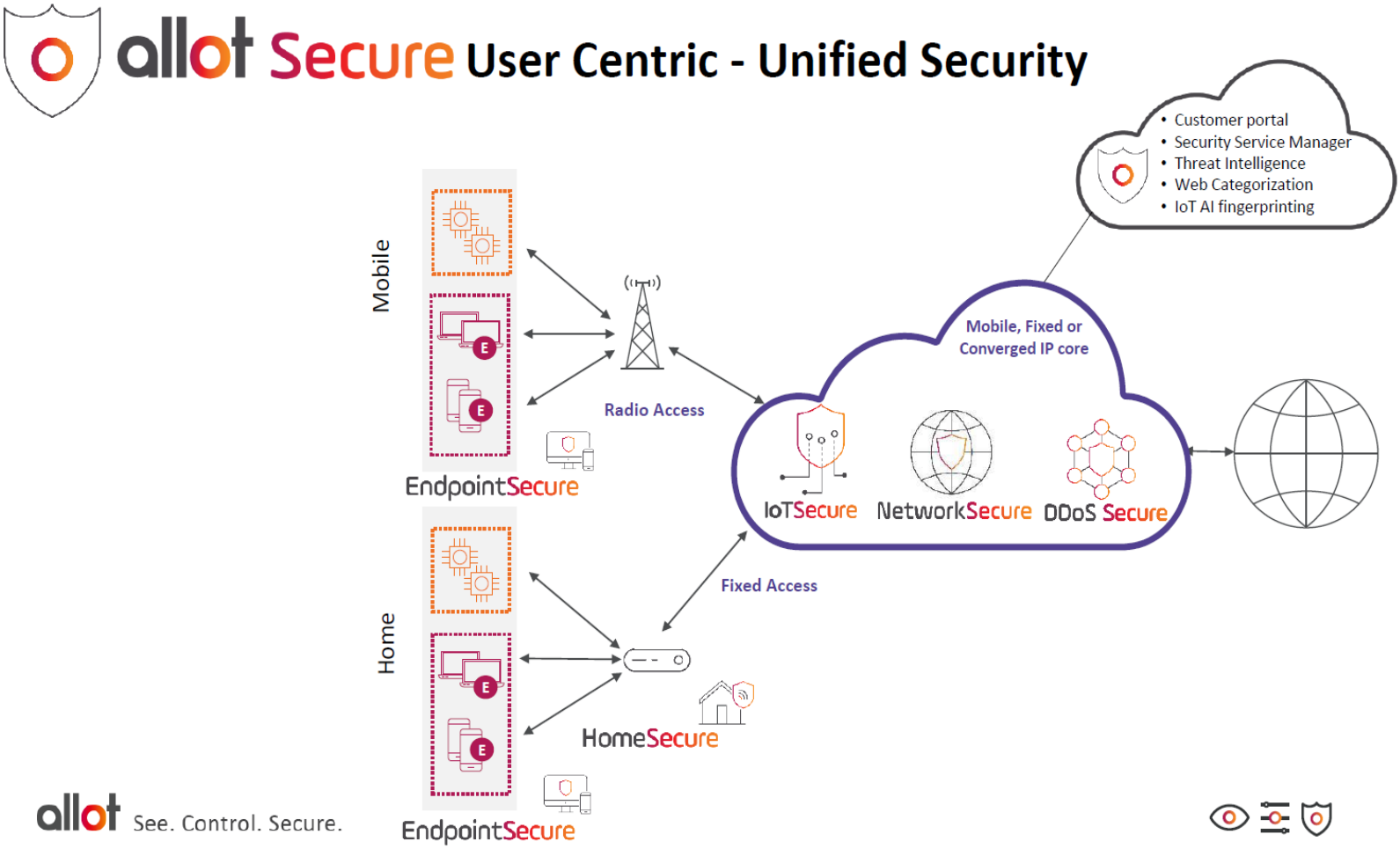
Allot Secure enables CSPs to offer security services to mobile, residential, and business markets that protect end user and IoT devices. It also protects the CSP networks and telco infrastructure themselves from threats such as DDoS attacks. The Allot secure platform includes 5 separate solutions which offer security for any application. They are detailed in the graphic below.

Allot Smart gives CSPs and enterprises the ability to see, control, and optimize network traffic to ensure delivery of services at a high QoE, while reducing both operational and capital expenditures.

Allot Secure

Allot secure is comprised of the following 5 platforms:

The diagram below shows where these products sit within the communications network:



AllotSecure products enable customers to deliver the following services:

●Content Filtering
Allot's global database of web categories enable consumer parental control and businesses to enforce acceptable-use policies. Content inspection is based on HTTP/S header inspection and does not rely on DNS, preventing the end-user from bypassing control by tunneling encrypted DNS requests to a 3rd party such as Google or Cloudflare.

●Web Security
Up-to-date threat intelligence and in-line anti-virus scanning protects users from malware such as crypto jacking, ransomware, and banking-trojans and devices from IoT specific attacks such as Mirai and its variants.

●IoT Security
In addition to network based anti-malware and web security, Allot Secure introduces carrier scale access control to block unsolicited communications that significantly impact IoT group data plans.

●DDoS Mitigation
Protect carrier infrastructure and customer networks from attacks that originate from external networks and from the access network. In-line, bi-directional mitigation coupled with DPI based Traffic Management enable accurate detection and mitigation, preemptive policies to protect critical network services, and detailed analytics for in-depth attack forensics.

●Anti-Phishing
Protects end users from falling victim to online scams that direct users to malicious websites that mimic legitimate ones in order to steal online credentials and/or infect the user's device with malware.

●Anti-Bot
Blocks bot "command and control" callback requests in-line, based on up-to-date threat intelligence, rendering bot infected endpoints dormant. This is effective for both IoT devices and endpoint devices since most bots avoid the use of DNS.

●Ads-Free
Blocks popup ads, animated gifs, and banners for a safer and nuisance free experience.

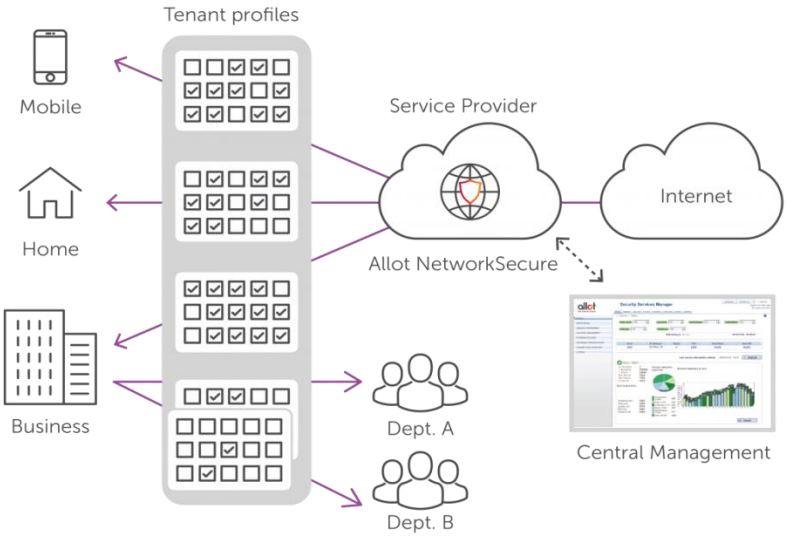
Network Secure

Consumers and businesses are becoming increasingly aware about the dangers of exposure to data theft, phishing attempts, ransomware and harmful content. With NetworkSecure, network-based security, CSPs can provide their own branded security service (SECaaS) and quickly scale to support and centrally manage security for tens of thousands of end users and businesses. Allot NetworkSecure is an integrated platform built for rapid rollout of personal security, parental control, and ads-free services that safeguard end users. It enables personalized security policies, event handling, and reports for

the mass market. It powers the world's largest deployed network-based security service, with over 20 million paying customers. Allot customer success teams engage with CSPs, helping them to plan, launch, and promote their security

service for maximum service adoption and retention. Several European Tier 1 service providers have already achieved more than 50% adoption rates by selecting Allot and Network Secure as their security service solution. Launching a mass informed "Try and Buy" campaign, for example, has achieved over 15% service adoptions in the first year. CSPs can simultaneously turn on the service for any, or all, customer segments generating revenue of around $1 or €1 per end user per month. There's no need for end users to download, install, or activate anything.

Network Secure supports many kinds of tenants. A tenant can be an individual, a family looking to apply parental control, or an organization securing its employees.



Families can use NetworkSecure parental control to apply simple security configuration settings that ensure their kids only view appropriate content and that they only use the internet for a limited time each day. Parents can also receive security alerts activated by their kids' online activity.

Small businesses are vulnerable to cyber-attacks, and typically lack in-house security skills. CSP delivered security gives small business owners peace of mind while keeping inappropriate content out of the workplace. Content can even be filtered based on specific departments and down to the individual user resolution.

Benefits to Customers

- Increase ARPU from consumer security services
- Maximize uptake through frictionless onboarding (users do not need to download any software)
- Safeguard children from dangerous and inappropriate content
- Strengthen customer loyalty with personalized notifications
- Add value to end users by protecting them against threats such as ransomware and crypto-jacking
- Gain valuable security and threat intelligence

HomeSecure

Allot's home security solution protects home devices from PCs, tablets, smartphones, IoT devices (security cameras to kitchen appliances), to the actual modem/router that provides connectivity. Many consumer-grade "smart" appliances are vulnerable, leaving the virtual door of the home network wide open. Allot's HomeSecure offers its customers a security service that protects the connected home which they can offer to end users to increase connectivity revenue by 10-15% without the need to replace existing CPE. By remotely integrating an Allot HomeSecure thin client with their CPE, customers are able to centrally manage all the security of end user connected devices. End users have per-device parental controls, and control over their home network through an intuitive app that keeps them engaged with their

home security. Parental controls can be applied per device or per a group of devices associated with each member of the household. HomeSecure parental controls are integrated with NetworkSecure so that they are set once and can be enforced for both mobile and WiFi access. The owner of the app will be notified about new connected devices attempting to join the network. The app owner can approve or deny access to the home network and manage connected devices.

Allot takes a multi-layered approach and provides additional protection with web security enforced at the CPE level, network-based A/V scanning, and lateral malware propagation to protect home devices from attacks originating from within the home network.

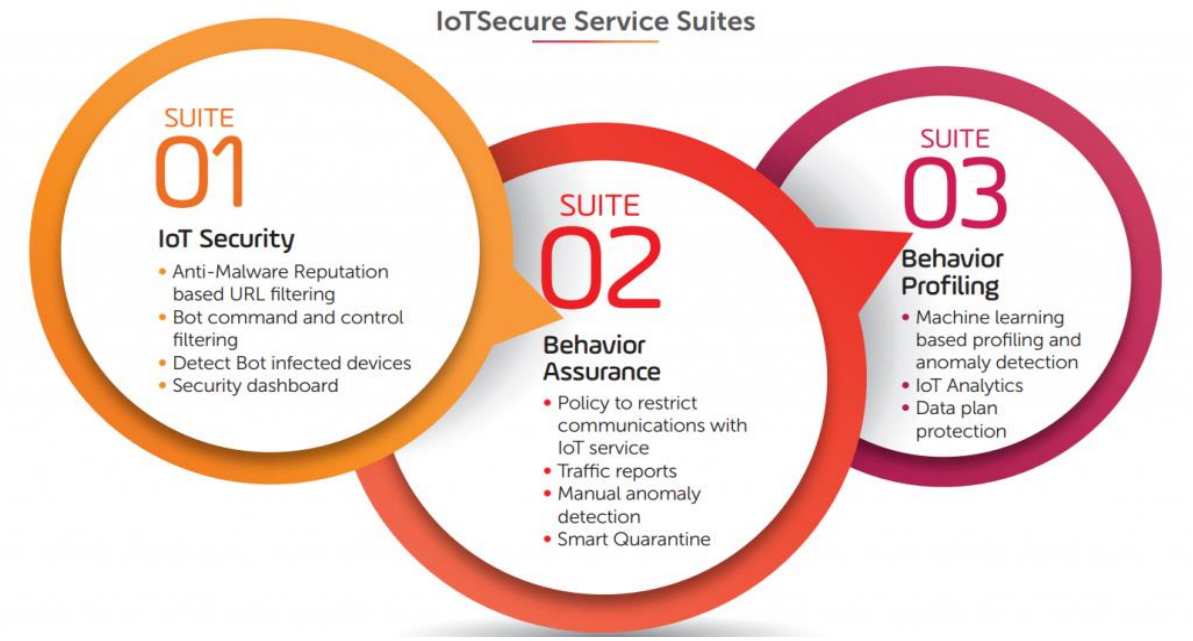
Benefits to Customers

- Add value to end users by protecting the connected home
- Increase average revenue per user (ARPU)
- Leverage existing install base of CPE and make them secure

IoTSecure

Machine-to-machine communications is already a significant business for mobile operators, and is set to grow when 5G networks go into mass production. And yet, from a cyber-security perspective, IoT devices remain vulnerable. Allot offers CSPs the ability to offer Security Value Added Services (VAS) that give enterprise users the means to confidently deploy mobile IoT devices at scale. This platform delivers carrier-class security, policy control, IoT analytics and behavior analysis that can be applied to any IoT service.

IoTSecure is based on a field proven solution that delivers security services today by Tier-1 mobile operators across the globe.



Benefits to Customers

- Provide IoT security services for any industry, leveraging core expertise
- Neutralize cyber-threats on IoT Infrastructure
- Leverage device and application-aware IoT analytics to troubleshoot, plan, and optimize IoT traffic
- Mitigate data plan abuse, miss use, and detect anomalies with IoT behavior profiling
- Generate an extra 15-20% revenue on top of connectivity charges
- Differentiation through a secure IoT offering

DDOS Secure

DDoS attacks are getting bigger, more frequent, and more sophisticated in their quest to flood networks and disrupt service availability. Allot DDoS Secure defends against both inbound and outbound attacks. It mitigates volumetric DDoS attacks and isolates infected hosts, before either can impact a network.

Allot DDoS Secure has highly scalable inline DDoS mitigation sensors that fully integrate with Data Packet Inspection (DPI) functionality. The solution inspects all traffic in and out to form accurate traffic behavior models and detect even the smallest attacks. Whether it's DoS/DDoS, attacks originating from IoT connected devices, outbound spam, worms or port scanning traffic generated by bot-infected users Allot DDoS secure defends against it. This means that customers can:

- Avoid rerouting traffic to scrubbing centers and save infrastructure costs
- Get always-on, bidirectional protection that responds in seconds not minutes
- Gain full automation with no need for supervision
- Cluster multiple sensors to thwart even the biggest volumetric attacks
- Neutralize zero-day attacks
- Prioritize critical traffic to maintain high Quality of Experience during attacks
- Deliver real time alerts and comprehensive attack forensics

Filter: Using dynamic filtering rules, the solution filters out attack packets and avoids over-blocking the network. This allows legitimate traffic to flow unimpeded, keeping customers online and protected at all times.

Pinpoint: By pinpointing the source of anomalous behavior, the solution quickly isolates infected devices at their source, and prevents them from serving as vehicles for cyber-attacks.

Real-time alerts: When a threat is detected and mitigated, customers are notified. Allot's detailed and customizable attack-mitigation logs, event analytics, host infection analytics, and trend/distribution reports will help to support customer security planning, threat management and operational decisions.

Benefits to Customers

- Detect cyber-attacks within seconds with no latency
- Maintain quality of service during attacks
- Eliminate traffic overload to maintain network efficiency
- Avoid being blacklisted as an attack or spam source

EndpointSecure: An extension of NetworkSecure, for securing end users off-net

Service providers in today's hyper-competitive market face the major challenges of attracting and retaining customers. The proliferation of devices used to access networks goes hand in hand with an escalation of security threats, because the attack surface has expanded. This provides an opportunity to provide differentiating security VAS. End-to-end security is built on the Allot NetworkSecure platform in the network, coupled with McAfee or BitDefender products on the endpoint. Together, they create one unified service that delivers on-net and off-net coverage to keep customers satisfied, and simple onboarding to accelerate service uptake and time-to-revenue. By combining the two into a single platform, complexity for the user is reduced, and a greater level of security is achieved.

Benefits to Customers

- Increase ARPU from consumer security services
- Drive customer satisfaction through differentiation
- Add value to end users by protecting them on and off-net

Allot Smart

Allot believes that when visibility is clear and network intelligence is accurate, service providers can make smart decisions in real time to manage their networks, engage customers and innovate with new services.

In today's challenging business environment, CSPs must use cost-effective measures to ensure the highest possible customer QoE to boost customer satisfaction and minimize churn. Allot Smart, powered by next-generation deep packet inspection (DPI) technology, generates insightful intelligence that empowers CSPs to optimize, innovate, and capitalize on every service opportunity. **By analyzing every packet of network, user, application, and security data, CSPs can see, control and secure their networks, optimizing performance, minimizing costs, and maximizing end-user QoE.** With a track record built on proven success with Tier-1 CPSs around the world, Allot Smart products enable CSPs to leverage their unique location at the crossroads of the connected world. Allot Smart extracts actionable intelligence from CSP networks, helping them deliver the best services that can:

- Save access bandwidth costs
- Defer capacity expansion
- Cut OPEX through automation
- Reduce revenue leakage

The Allot Smart platform is powered by the following products:

Allot Service Gateway – Unified platform for traffic monitoring, QoS, charging, steering and value-added services. The Allot service gateway is the product that is the base for all other Allot products. It is the single point of integration for network intelligence, policy control, traffic management, cyber threat protection and VAS. Allot Service Gateway platforms are designed for deployment in a wide range of networks both on traditional and virtualized network access infrastructure.

ClearSee – Real-time monitor/data analytics; presenting enriched application, subscriber, device, security and QoE data. Assuring network performance and quality of experience for end users requires a thorough understanding of who

and what is connected to a network, what applications are running, what resources they are consuming and when. Allot ClearSee Network Analytics gives clear visibility of network traffic, to ensure it meets users' expectations.

NetXplorer - Centralized Network Management System (NMS) for policy creation, traffic management, and platform and software configuration and maintenance.

SMP – Subscriber Management Platform for user-level visibility, enabling policies to be deployed at the user level

These Allot Smart products provide deep, granular visibility into both the subscriber and data planes. Advanced machine learning software analyzes and correlates this information to generate actionable intelligence that drives automated solutions for the following key domains:

- **Network Visibility** – SmartVisibility provides actionable network intelligence to make informed business decisions
- **Traffic Management** – SmartTraffic QoE monitors and controls network traffic, within budget, to deliver optimal QoE
- **Policy & Charging Control** – SmartPCC delivers and enforces innovative service plans across any platform
- **Regulatory Compliance** - SmartRegulator meets regulatory requirements with flexibility and precision

Below are some of the key features of these domains:

Accurate Traffic Visibility and Policy Control

Allot's Dynamic Actionable Recognition Technology (DART) engine, embedded in the Service Gateway employs multiple deep packet inspection (DPI) and analytical methods to identify network traffic by subscriber, application, device and network topology. The technology is able to identify a plethora of Over-the-Top applications with frequent and custom updates to Allot's extensive signature library. These elements can be used directly for dynamic traffic management, and charging and service enablement policies.

Encrypted Traffic Classification

In order for the Service Gateway to see, control, and secure data, it must be able to see what that data is. Today, much of the data that passes through our communication networks is encrypted and therefore difficult to classify. Allot's traffic classification proactively learns and adapts to the changing tactics of traffic encryption that are widely used by Internet services and data privacy applications. From heuristic analysis of IP flow behavior to peer learning and predictive DPI, Allot's synergy of inspection methods provides highly granular and accurate recognition of encrypted traffic even at maximum speeds and peak loads.

Intelligent PCEF/TDF

Simply put, these features ensure that end users are billed correctly and that CSPs can highly customize the way they bill end users. Allot's Service Gateway provides intelligent Traffic Detection Function (TDF) and Policy and Charging Enforcement Function (PCEF) in mobile data networks. As a result, network operators can leverage Allot's granular traffic classification and metering to enrich policy decisions and to enhance the charging capabilities of online and offline charging systems (OCS, OFCS). This gives CSPs the flexibility to offer packages such as: zero-rated apps, VoIP plans, bite-size data services, emergency credit, try and buy, gifting, app roaming plans, and tethering plans.

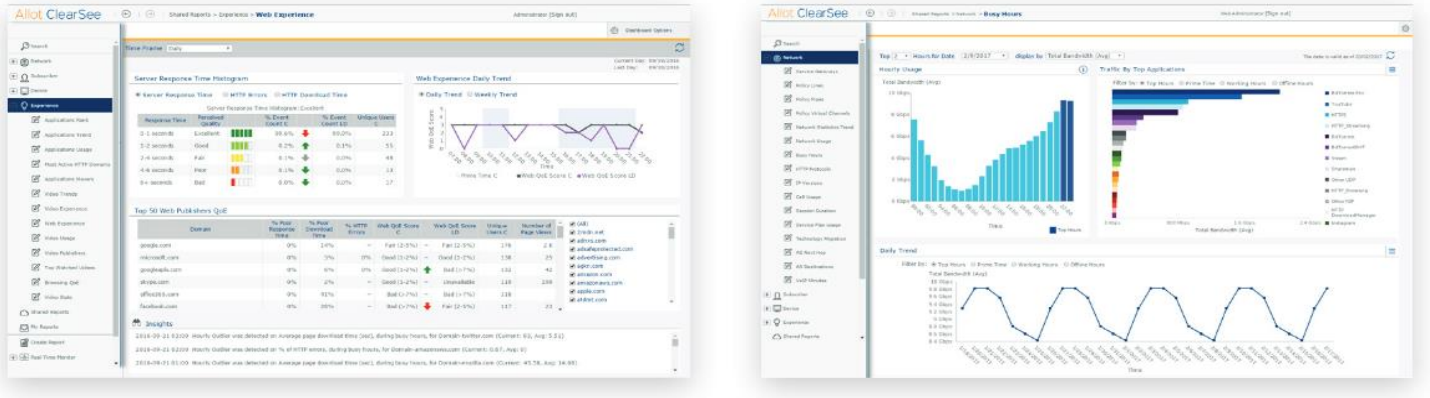
Data Centric

Network service performance and user satisfaction are key to business success. The ability of CSPs to obtain meaningful business intelligence from their network usage data is key to making the right business decisions. From its vantage point in the network, the Allot Service Gateway collects and exports a rich variety of high-resolution usage data, including real-time transactions per user, per application, per device, per video session, per VoIP and Instant Messaging session, per Web session, and more. Network data records may be exported in standard formats to business intelligence systems, such as Allot ClearSee Network Analytics, and other operator systems for further manipulation and analysis. Frequency and triggers for data record export are configurable parameters, giving operators ready access to usage data that is critical to their business.

Allot ClearSee Analytics helps network operators turn this big data into valuable insight for the decision-makers in their organization. It is a complete toolkit for seeing and understanding everything that is happening on a network. Reporting dashboards are organized per domains that are of interest to every network operator – Network, Subscriber, Device, Experience and Security. All dashboards are under the same pane of glass, so customers can easily switch back and forth between real-time views and longer-term metrics.

Analytics Domains	Reporting Dashboards
Network	Real-time health, Congestion analysis, Busy Hour, Peak Period, Application usage/popularity, Signaling analysis, and more
Subscriber	App usage, Device usage, Content consumed, Video and VoIP usage, QoE metrics, and more
Device	Data volume, App usage per model, 3G vs 4G, and more
Experience	Top content, Top consumers, Top publishers, Video and HTTP QoE per app/sub/device, and more
Security	Security dashboards display web activity, threat events, and blocked targets reported by Allot parental controls, anti-virus, anti-phishing, antispam, and firewall services

With these resources network operators can learn how their customers behave, establish emerging network usage patterns, and identify challenges slowing down their network. They then transform this data into valuable business intelligence that helps them plan and take action to achieve their business goals.



Network Metrics Dashboards

For example, real-time reports can show which applications and devices are consuming the bandwidth in a chronically congested cell, while historical analysis can be used to identify traffic trends and the effects they will have on network performance over time. Daily or weekly reports showing bandwidth consumption, usage volumes, video and HTTP QoE, signaling traffic, average bitrates, sessions opened, and other vital statistics enable operators to identify problematic areas and better plan around them.

This data centric approach allows CSPs to:

- 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
- Deploy personalized service plans for individuals and groups
- Evaluate the performance of tiered and quota service plans

Marketing professionals gain the ability to quantify and characterize subscriber activity to assist with customer segmentation and service planning. For example, analysis of subscriber-application-device usage can be used to target customers most likely to respond to a service plan upgrade, thereby improving response rates and increasing customer lifetime value. Using the system's flexible self-service approach, marketeers can build their own reports to explore usage trends and outliers on the fly.

Executive Management gain from a consolidated view of their network business provided by report dashboards that summarize the key performance indicators they want
to track - for example – monitoring the adoption and performance of newly launched services per demographic or per location. Web-based dashboards may be viewed on multiple devices from any location.

Self-Service Data Mining

Allot does not limit customers to a predefined set of reports or a specific way to analyze data. As new requirements arise, or new data presents itself, the Self Service analytics module helps customers model their questions and find answers to complex business problems such as discovering new market and service opportunities before the competition, or gaining insight on how to dramatically improve customer satisfaction and retention rates. While the Self-Service module is easy to use, it provides an excellent tool for experienced analysts who for the first time have access to source data that is more varied, detailed and accurate than ever before. Custom, ad hoc analyses and reports can be built without the need for software development or upgrade. Changes and what-if scenarios can be tested on the fly. With Self-Service, customers can find answers to specific questions, explore possible courses of action, and often discover problems and opportunities that were not anticipated.

QoE Optimization

The increasing volume of data traffic is a constant challenge to CSPs that have to provide enough capacity to fulfill demand and Quality of Experience (QoE) expectations. CSPs know that adding more bandwidth is not cost effective in the long run. Regardless of the bandwidth provided, end users will demand more. If a CSP chooses to make capacity investments they are not backed by an increase in ARPU. Network capacity is still vital to enable good QoE, but it is how this capacity is used that determines the level of QoE. This is why congestion control solutions are key in order to create network efficiency.

QoE is personal. That's why Allot monitors the quality of individual connections (QoE indicators) together with specific locations in the network, such as within a mobile cell, a BRAS interface, DSL interface or a CMTS channel/bonding group.

While mobile operators have invested millions to deliver reliable QoE to their customers, every mobile cell has its limits. Ideally, traffic demand in a mobile cell should not exceed what the cell can deliver. Otherwise, voice and data sessions are dropped. But in real life, the available bandwidth in a given cell at any given time is practically unknown. Anything from IMS and video calls, which consume significant bandwidth, to changing weather conditions can reduce cell capacity in an instant, making cell service more susceptible to congestion and QoE degradation.

Allot provides a solution by enabling mobile operators to assess the available bandwidth in any given cell at any time, based on QoE indicators. It measures what users in the cell are actually experiencing in real time and automatically triggers QoE policy to shape consumption while allocating the available bandwidth according to the operator's traffic policy. Accurate assessment of the available bandwidth in a cell plus real-time QoS policy enforcement on the traffic of users in that cell, requires mobility information from the network. Allot Service Gateway obtains real-time mobility information over standard interfaces so it can enforce QoE Congestion Management policy per cell-user in tandem with changing cell conditions and users moving in and out of coverage. In parallel, mobile operators can use Allot ClearSee Network Analytics to identify recurring patterns and possible trends involving TCP RTT and retransmission metrics, so that if a certain cell is frequently over-utilized it can be upgraded to accommodate the demand. With Allot solutions, cell congestion is kept under control and mobile operators are able to deliver a consistently good user experience that keeps subscribers satisfied and loyal.

Cable networks have a unique congestion challenge which is fueled by commonly used oversubscription models. It is not unusual for high bandwidth demand from a few people using P2P, video streaming, or file sharing applications to degrade cable service on a particular street or in a whole neighborhood, ruining the online experience for everyone sharing the cable access resource. Unlike DSL and wireless networks, the available bandwidth in cable network is known at every given moment and can be obtained from CMTS elements in order to adjust bandwidth demand accordingly. Allot is able to monitor available bandwidth at the most granular level of a CMTS channel and/or CMTS bonding group. These represent various groupings of multiple homes, multiple streets, subdivisions, neighborhoods, etc. Allot monitors and measure the discrepancy between available bandwidth and demand on each channel or bonding group, and

automatically triggers application-aware and user-aware QoS controls until congestion is alleviated and quality of experience is restored.

Customers are in control of simple policy management that they can configure themselves to assure the quality of experience their network delivers to every user. They leverage:

- Ability to assure QoE on any network access and across converged networks
- Carrier-grade scalability that assures QoE for millions of users
- Multiservice platform that also provides Network Intelligence, Policy and Charging Control, Traffic Management, Network Security, and VAS Delivery

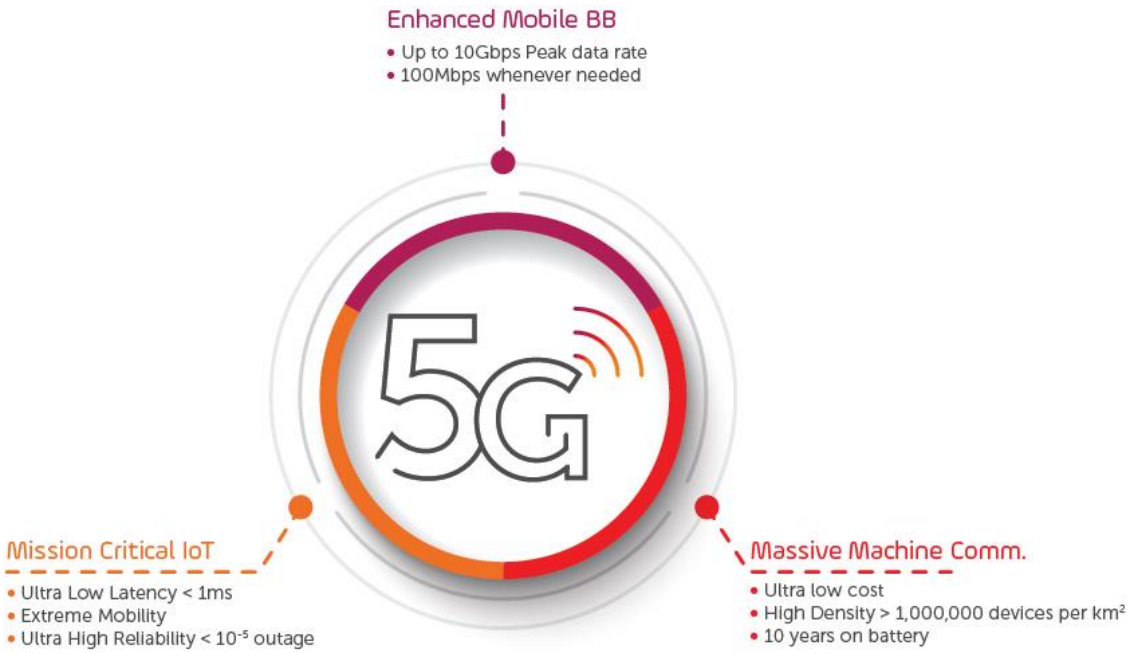
5G Slicing

5G takes mobile network evolution to a new level with service-based networking that supports massive IoT growth, fixed-mobile-convergence and critical machine-to-machine (M2M) communication.

End-to-end network slicing, enabled by NFV, supports different services by dynamically allocating virtual resources and functions to meet service-specific performance objectives. The Allot Service Gateway Virtual Edition (SG-VE) and NFV manager comply with leading NFV orchestration systems and are 5G ready.

The three main use cases for 5G are Extreme Mobile Broadband, Massive Machine Communication, and Critical Machine Communication. These three services demonstrate the versatility of 5G networks on the vectors of scale, throughput, and latency. 5G drives fixed-mobile convergence and the massive growth of endpoint connectivity.

For example, a single 5G network is capable of supporting 8K video streaming, gaming, and virtual reality in addition to ultra-reliable, low latency, low bandwidth, V2X collision avoidance systems and other machine-to-machine communications, on a massive scale.



Supporting all services with such high performance objectives on one monolithic network would be extremely cost prohibitive. 5G addresses this with end-to-end network slicing, ensuring that each network slice can support a service and its specific performance objectives. Network slicing is a form of virtualization that allows networks to run on top of a shared physical infrastructure so that a CSP can provide 5G services but at the same time not transfer their whole network to 5G standards as this is CAPEX intensive. In this way, just a slice of the network supports 5G.

Network slicing relies on virtualization of physical resources and network functions, and the employment of advanced network management and orchestration systems. The network allocates resources and their placement in the network to meet the performance objectives for each slice and its associated service. The network dynamically scales network function resources up or down to adapt to changing traffic conditions

Quality Assurance- The SG-VE augments standard 5G technical performance indicators through a customer-centric approach that considers Key Quality Indicators (KQIs) to ensure end-user quality of experience (QoE). For example, it looks at resolution and stalls when assessing perceived video QoE to achieve highest customer satisfaction in addition to optimal resource utilization.

Service Differentiation- A second benefit of the SG-VE is more granular (e.g. application specific) visibility and control. Within a Mobile broadband (mBB) slice, you may want to differentiate by criteria such as applications, content providers, users, and locations. For example, in a slice that provides both streaming video and cloud backup, stalls will significantly impact the video QoE, but not the cloud backup. With the SG-VE you can optimize accordingly.

Network Protection- With 5G's increased access rates and massification of IoT, attacks from the radio access network can be devastating. Allot's carrier-class DDoS detection and mitigation solution holistically addresses the three phases of a DDoS attack; the compromise or infection of endpoints, the weaponization of the endpoint, and the DDoS attack itself. Critical network resources and user QoE are assured, even during an attack.

Regulatory Compliance

Regulatory compliance has become mission critical for national authorities and Communication Service Providers (CSPs) due to increased cyber threats such as offensive, criminal or unethical on-line activities, and attacks on communications infrastructure. Regulations aimed at protecting the general population often require network operators to capture, analyze and retain records of application usage, block harmful content and sites and safeguard communication infrastructures against denial of service attacks.

Law enforcement and homeland security agencies rely on service providers to lawfully intercept, block and record dangerous traffic to help mitigate internal and external criminal and security threats. To meet these requirements, service providers need a flexible, powerful and scalable solution that resolves current and future threats through adaptive machine learning of malicious behavior and dynamically expanding threat identification.

Allots solution blocks illegal content such as pornography, violence, drugs, child abuse, fake and untruthful content and illegal applications. It provides unlimited retention of detailed usage records and protection of network infrastructure against DDoS attacks. It is specifically designed to enable CSPs to meet national law enforcement and/or homeland security authority requirements and consists of following main components:

Security

- DDoS detection and mitigation of volumetric inbound and outbound based on advanced Network Behavior Anomaly Detection (NBAD) technology
- IoT Botnet activity detection and containment
- Detailed threat intelligence on attackers and their targets in the network
- High-precision blocking of illegal Anonymity and VPN applications utilizing machine learning algorithms
- Privacy by design ensuring confidentiality of personal data and restricting access to authorized users

Network Intelligence

- Industry leading DPI traffic awareness overcomes data encryption
- Automatic analysis and classification of application, user, session, device, location, content, type of interest and more
- Built-in support for thousands of applications and protocols - expandable through automatic updates or self-service interface
- Detailed extraction of Web traffic information and storage online usage records
- Unified front-end GUI integrates all data sets, and enables self-service analysis to produce meaningful intelligence such as user browsing behavior, destinations, and trends

Application and Content Filtering

- Precise, encryption agnostic URL classification and illegal URL filtering
- Supports global IWF blacklist as well as import of blacklist policies from national regulatory bodies
- Varied content management actions including block, redirect and disrupt (rate-limit) traffic to specified sites

Data Retention

- Scalable and reliable big data warehouse for long retention of high volume data records
- Built-in high availability
- Simple interface for ad-hoc retrieval of user online web log

QoE for Enterprise

Allot helps assure exceptional QoE for business-critical apps. If a network is slow and end users are complaining, Allot real-time network monitoring & metrics can show customers how every application and user is behaving on their network. When datacenter and cloud applications don't perform as expected, businesses can suffer from low user satisfaction, slow adoption, and inability to operate efficiently. Moreover, with ubiquitous BYOD and Internet access in campus and branch locations, networks becomes a conduit for all kinds of traffic that may be crowding out critical apps. Allot's solution classifies and quantifies all the activity on a network so its customers can take the right steps to ensure consistent and reliable performance of their applications.

The DART signature library and customizable policy elements let customers monitor and measure application performance and user Quality of Experience with very fine granularity, so they can quickly zero in on network problems and troubleshoot faster.

Customers can:

- Identify shadow IT and anonymity apps competing for network resources
- Pinpoint root causes of LAN, WAN, Internet congestion
- Identify potential problems before they occur
- Create control policies in accordance with insights

Accurate 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. 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.

Allot's synergy of inspection methods results in highly granular and accurate recognition even at maximum speeds and peak loads. DART proactively learns and adapts to the changing tactics of services and applications that use encryption, by using:

- Pattern and numerical property analysis of packet contents.
- Heuristic analysis of behavior statistics from inspected transactions.
- Peer learning: analysis of peer system behavior to identify P2P seeders (multiple transmission of files) and popular peers
- Port, IP address, or range of IP addresses classification
- Machine learning based on statistical distribution patterns for over 1000 traffic attributes
- Automatic IP discovery through analysis of service hosts and subscriber records
- Predictive DPI (PDPI): Allot's patented technology that enables the classification engine to learn from the patterns and behavior of traffic that it recognizes with 98% accuracy, and compare them to encrypted flows in order to improve identification.

Financial Valuation and Projections:

Financial Analysis

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 telecom 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.

22% and 32% of total revenues in 2018 and 2017 respectively were derived from one Tier 1 mobile and fixed operator. In 2016, 42% of total revenues came from two Tier 1 mobile and fixed operators.

On the year ended December 31, 2018 product revenues increased by $7.3 million, or 14.9%, to $56.2 million in 2018 from $48.9 million in 2017. The increase in revenues in 2018 was attributable to better execution capability, changes in Company structure to better support sales efforts, and higher demand for the Network Intelligence offering.

Service revenues increased by $6.4 million, or 19.3%, to $39.6 million in 2018 from $33.2 million in 2017. A material part of the service is linked to the sale of products; thus, service revenues increased in correlation with product revenues.

Cost of revenues and gross margin: Cost of product revenues increased by $0.8 million, or 4.2%, to $20.1 million in 2018 from $19.3 million in 2017. Product gross margin increased to 64.3% in 2018 from 60.5% in 2017. This increase is attributed to increase in revenues. Cost of services revenues increased by $0.02 million, or 0.2%, to $9.3 million in 2018 from $9.3 million in 2017. Total gross margin increased to 69.4% in 2018 from 65.2% in 2017.

Exploring the second quarter of 2019 indicates the following:

- **Total revenues** for the quarter were $26.6 million, an increase of 15% compared to $23.0 million in the second quarter of 2018.
- **Gross profit on a non-GAAP basis** for the quarter of was $18.5 million (gross margin of 69.8%), a 12% improvement compared with $16.6 million (gross margin of 72.2%) in the second quarter of 2018.
- **Non-GAAP operating loss** for the quarter was $2.1 million, compared with a non-GAAP operating loss of $1.3 million in the second quarter of 2018.
- **Non-GAAP net loss** for the quarter was $2.1 million, or $0.06 per basic share, compared with a non-GAAP net loss of $1.2 million, or $0.04 per basic share, in the second quarter of 2018.
- **Cash and investments** as of June 30, 2019 totaled $101.6 million.

Valuation

Valuation Methodology:

Growth company valuations are challenging due to a non-cash / limited cash flow valuation with a long time-to-market in most cases. Methods typically used for company valuations, such as asset valuation or multiplier methods, are incompatible with the valuation of growth companies. In such companies, the current status of business cannot be analyzed by the capital in the balance sheet, and in most cases cannot be compared to similar companies due to their uniqueness, in both technological and financial aspects.

As part of a discounted cash flow (DCF), the accepted method used in financial valuations, there are several modifications to a growth company's valuation. In general, there are three primary methods within the DCF method:

1. **Real Options** - valuation method designated for pre-clinical and early-stage clinical programs/companies where the assessment is binary during the initial phases and based upon scientific-regulatory assessment only (binomial model with certain adjustments).
2. **Pipeline assessment** - valuation method used for programs/companies prior to the market stage. The company's value is the total discounted cash flow plus unallocated costs and assessment of future technological basis. The assessment of the future technological basis is established based on the company's ability to "produce" new clinical and pre-clinical projects and their feed rate potential.
3. **DCF valuation** - similar to companies not operating in the life sciences field, this method applies to companies with products that have a positive cash flow from operations.

Allot's valuation was conducted under the DCF valuation method, while the Network Security business was analyzed under a growth model, as a relatively new business.

Company valuation

Allot revenues are mainly based on products and services, however a better view, in our opinion is on two separate lines of business operating in two different however integrated domains: Network Intelligence (DPI) and Network Security.
We forecast, in our 7 year forecast, two revenues streams: One for Network Intelligence (DPI) and one for Network Security with different CAGRs based on the potential of Allot as described below in these two markets.

- DPI revenues: Allot announced (Sep. 16, 2019) that it has entered into a significant agreement to provide AllotSmart products to an existing customer located in the EMEA region for total consideration of tens of millions of dollars. Allot expects to receive a portion of the amount as an advance payment, with the revenues expected to be recognized over several years and are subject to customary delivery and acceptance terms. Margins of the deal are similar to Allot's average margins. Thus, we assume some growth in 2020-2021 and a steady growth from 2022 to our future forecast. Based on our understanding the whole market will enter into a steady state in the coming years as DPI market potential according to our analysis and Allot's management view has already experienced somewhat of a peak. We assume 5% CAGR in our future forecast.

- Security revenues: we see this market in its early life cycle with higher CAGRs and with a great potential for growth. We analyze the company's maximum annual revenues from its clients and assume $27 million by the end of 2019 and then an annual two digit growth rate as can be seen in the table below.

Gross profit was an average of 68% in 2016-2018 with some growth in 2018. We assume mild growth mainly due to clients' movement to cloud based services in the coming years.

Operating expenses:

- Selling and marketing - will continue to be in the range of 40% to 43% of revenues in linear correlation with revenues in order to support growth.
- Research and development – as Allot needs to support its efforts in the security domain, will remain high at a 10%-12% annual growth rate.
- Operating profit – we assume breakeven in late 2021/early 2022.
- General and administration – we assume a constant (and high) growth rate of 5% annually.

Below is our forecast for 2019 – 2024:

$, 000		2016A	2017A	2018A	2019E	2020E	2021E	2022E	2023E	2024E
DPI			57,900	71,337	82,087	94,400	103,840	109,032	114,483	120,207
YoY growth				*23%*	*15.1%*	*15.0%*	*10.0%*	*5.0%*	*5.0%*	*5.0%*
Network based security			24,129	24,500	26,950	30,993	54,461	94,522	144,792	202,633
YoY growth				*2%*	*10.0%*	*15.0%*	*75.7%*	*73.6%*	*53.2%*	*39.9%*
Total revenues		**90,533**	**82,029**	**95,837**	**109,037**	**125,392**	**158,301**	**203,553**	**259,275**	**322,840**
YoY growth					*13.8%*	*15.0%*	*26.2%*	*28.6%*	*27.4%*	*24.5%*
Cost of revenues		26,251	26,288	28,086	31,188	36,121	44,809	57,618	73,391	91,384
Gross profit		**64,282**	**55,741**	**67,751**	**77,849**	**89,271**	**113,492**	**145,935**	**185,884**	**231,456**
% of revenues		*71.0%*	*68.0%*	*70.7%*	*70.7%*	*71.2%*	*71.7%*	*71.7%*	*71.7%*	*71.7%*
Operating expenses:										
Selling and marketing expenses		32,289	34,740	38,959	44,803	51,523	63,320	79,386	101,117	125,908
% of revenues	*15%*	*36%*	*42%*	*41%*	*41%*	*41%*	*40%*	*39%*	*39%*	*39%*
Research and development expenses		22,629	20,889	24,415	28,077	32,289	37,132	42,702	49,107	56,473
% of revenues	*15%*	*25%*	*25%*	*25%*	*26%*	*26%*	*23%*	*21%*	*19%*	*17%*
General and administrative expenses		9,002	8,735	9,187	9,830	10,518	11,044	11,597	12,176	12,785
% of revenues		*10%*	*11%*	*10%*	*9%*	*8%*	*7%*	*6%*	*5%*	*4%*
Total operating expenses		63,921	64,364	72,561	82,710	94,330	111,497	133,684	162,401	195,166
% of revenues		*71%*	*78%*	*76%*	*76%*	*75%*	*70%*	*66%*	*63%*	*60%*
Operating (loss) profit		**361**	**-8,623**	**-4,810**	**-4,862**	**-5,059**	**1,995**	**12,251**	**23,483**	**36,290**

Other parameters:

- Tax – we assume, based on our tax model, the company will use its carry forward tax.
- Working capital – based on actual data (2016-2018) we assume constant pace.
- CapEx – we assume CapEx will be similar in our model to depreciation.
- Capitalization rate – based on our CAPM model (see appendix B) we assume CAPM of 17.8%.

Equity Value

Non-operational assets/liabilities and unallocated costs

As of June 30, 2019, Allot has non-operational assets (cash) of approximately $101 million. The company has $0.5 million in loans as of June 30, 2019.

Based on the above parameters we evaluate Allot's equity value at $411.8 million/1.43 billion NIS.

Sensitivity Analysis

The table below presents Allot's equity value in relation to the capitalization rate. We set a range of 1% change from our CAPM model (see Appendix B).

Sensitivity Analysis - Capitalization Rate vs. Target Price

Cap. rate	Target Price (NIS)
19.8%	42.4
18.8%	**42.0**
17.8%	**41.8**
16.8%	**41.7**

We estimate Allot's price target to be in the range of 41.7 NIS to 42.0 NIS with a mean of 41.8 NIS.

Appendices

Appendix A - Financial Reports

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,	
	2019 (Unaudited)	2018 (Unaudited)	2019 (Unaudited)	2018 (Unaudited)
Revenues	$ 26,554	$ 23,003	$ 51,896	$ 44,735
Cost of revenues	8,301	6,712	15,594	13,636
Gross profit	18,253	16,291	36,302	31,099
Operating expenses:				
Research and development costs, net	7,633	6,298	14,807	12,091
Sales and marketing	11,209	10,182	22,686	20,215
General and administrative	923	2,579	3,628	5,045
Total operating expenses	19,765	19,059	41,121	37,351
Operating loss	(1,512)	(2,768)	(4,819)	(6,252)
Financial and other income, net	571	806	1,103	1,036
Loss before income tax expenses	(941)	(1,962)	(3,716)	(5,216)
Tax expenses	592	455	1,150	887
Net Loss	(1,533)	(2,417)	(4,866)	(6,103)

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

	June 30, 2019 (Unaudited)	December 31, 2018 (Audited)
ASSETS		
CURRENT ASSETS:		
Cash and cash equivalents	$ 17,517	$ 16,336
Short term deposits	17,624	22,543
Restricted deposit	506	465
Marketable securities	65,681	64,290
Trade receivables, net	21,863	26,093
Other receivables and prepaid expenses	4,552	3,647
Inventories	10,687	11,345
Total current assets	138,430	144,719
LONG-TERM ASSETS:		
Restricted deposit	257	257
Severance pay fund	357	345
Operating lease right-of-use assets	6,129	-
Deferred taxes	463	281
Other assets	877	600
Total long-term assets	8,083	1,483
PROPERTY AND EQUIPMENT, NET	7,385	6,249
GOODWILL AND INTANGIBLE ASSETS, NET	35,802	37,393
Total assets	$ 189,700	$ 189,844
LIABILITIES AND SHAREHOLDERS' EQUITY		
CURRENT LIABILITIES:		
Trade payables	$ 6,601	$ 7,813
Deferred revenues	15,271	13,855
Short-term operating lease liabilities	2,480	-
Other payables and accrued expenses	21,473	21,052
Total current liabilities	45,825	42,720
LONG-TERM LIABILITIES:		
Deferred revenues	4,154	4,247
Long-term operating lease liabilities	4,031	-
Accrued severance pay	768	806
Other long term liabilities	590	6,168
Total long-term liabilities	9,543	11,221
SHAREHOLDERS' EQUITY	134,332	135,903
Total liabilities and shareholders' equity	$ 189,700	$ 189,844

Appendix B - Capitalization Rate

Cost of equity capital (ke) represents the return required by investors. The capitalization rate is calculated using the CAPM (Capital Asset Pricing Model). It is based on a long-term 10-year T-bond with a market risk premium, and based on Professor Aswath Damodaran's (NY University) commonly used sample (www.damodaran.com). As of January 2019, the US market risk is estimated at 5.69%. A three-year market regression unleveraged Beta is 1.25, according to a sample of 44 companies representing the US software firms. We used an unleveraged beta of this sample, which is higher than a leveraged beta, due to high rate of cash versus debt. The implied CAPM is 7.6%.

CAPM model (ke) is estimated as follows: $ke = rf + \beta(rm-rf) + P$

Allot is a small cap company, under $2b, in which marketability and size premiums need to be considered. Duff and Phelps' data research in the years 1963-2018 indicates that a 10.24% premium needs to be added to the CAPM for small cap companies. We therefore estimate the company's CAPM to be 17.8%.

CAPM Model		Value	Source
Long-term (20 years) T-bond	R(f)	0.46%	US Department of the Treasury (20Y)
Market risk premium	R(m)- R(f)	5.69%	based on Professor Damodaran's sample (1/19)
Beta unleveraged	B	1.25	Beta sample of 44 software firms (1/19)
Cost of Capital	Ke	7.6%	
Size Premium		10.24%	Duff and Phelps data, 10dz.
CAPM	CAPM	**17.8%**	

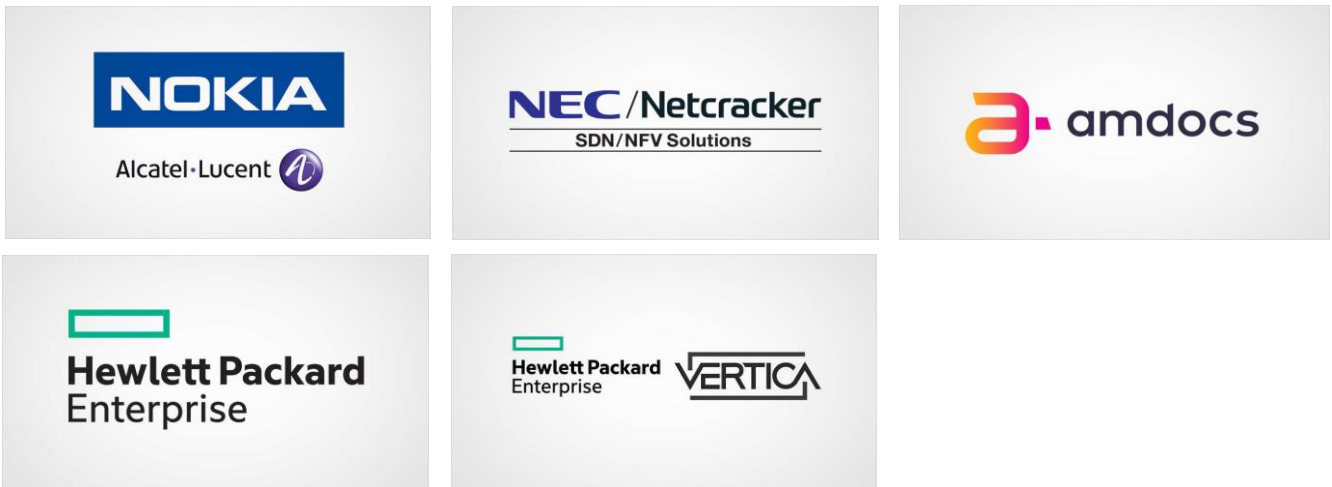
Appendix C: Partners

Solution Partners:

Allot partners with industry leaders in order to deliver some of the highest grade integrated solutions available in the market.

Technology Partners:

Allot partners with technology leaders of all sizes to provide optimal solutions.



FROST & SULLIVAN

Credit to Experts: Deepali Sathe, 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

Some of the other companies we cover:

EnteraBio, BIOLINERX, KADIMASTEM stem cells to cure diseases, Brainsway, enlight, CELLECT, D.N.A Biomedical Solutions, itamar medical, oramed Pharmaceuticals Inc, ENERGIXGROUP CREATING YOUR GREEN ENERGY, ELECTREON CHARGING THE WAY FORWARD

FROST & SULLIVAN

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. The fees shall be in the range of 35 to 50 thousand USD per each participant. 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.