allot
See. Control. Secure.

Actionable Intelligence & Innovative Security

Service Providers

EXECUTIVE SUMMARY

Communication Service Providers (CSPs) are challenged by flat or declining ARPU. Competition and churn are a constant concern. Over-The-Top (OTT) applications cut heavily into traditional revenue sources. How can you turn this around and deliver attractive services, reduce your operational expenses and defer capital expenditures associated with infrastructure expansion?

Allot's multi-service gateway combines Actionable Intelligence with Innovative Security Value-added-Services to meet and solve these challenges.

Our Allot Smart solution suite, powered by inline DPI technology, generates actionable intelligence that empowers you to optimize, innovate, and capitalize on every service opportunity. By analyzing every packet of network, user, application and security data, Allot Smart cost-effectively enables the highest Quality of Experience (QoE) for your end-users.

Allot Secure, our network-based security platform, disrupts the security industry by positioning CSPs as leading Security-as-a-Service providers, with market penetration exceeding 50% and protecting over 20 million subscribers worldwide. Allot Secure protects mass market mobile devices and enables CSPs to secure enterprise and consumer IoT deployments at the network layer, in fixed, mobile and converged networks.

Allot solutions enable CSPs to:

- Turn detailed network, user and application visibility into actionable insights that optimize service packaging
- Effortlessly incorporate value-added services to speed up monetization
- Deliver network-based end-user security that generates revenue and strengthens brand
- Secure home and enterprise IoT devices
- Automatically optimize traffic, deferring the need for costly network expansion
- Intelligently block known and unknown DDoS attacks
- Smoothly meet regulatory requirements for URL filtering and usage data retention

Common CSP use cases include application analytics, traffic control and shaping, network-based security services, regulatory compliance and more. We are deployed at over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our revolutionary network-based security as a service solution has achieved over 50% penetration and is already used by over 20 million subscribers in Europe.

Monetizing Security as a Service

Network-based security for mobile, home and office devices.

Built-in customer engagement tools; drives 50% adoption rates and revenues of 1-2 euro per month/per subscriber.

Actionable Intelligence for QoE

Layers 4-7 traffic visibility, including encrypted applications via 100% identification APIs, automates policy-driven congestion management to deliver optimal QoE.

DDoS Mitigation & Bot Containment

Bidirectional, large scale, real-time DDoS mitigation of attacks from outside and inside your network.

Monitors 100% of traffic and uses AI to identify & block zero-day attacks.

IoT Security

Network-based, proven, carrier-class security, behavior analysis and traffic intelligence and control – configured through a customer portal.

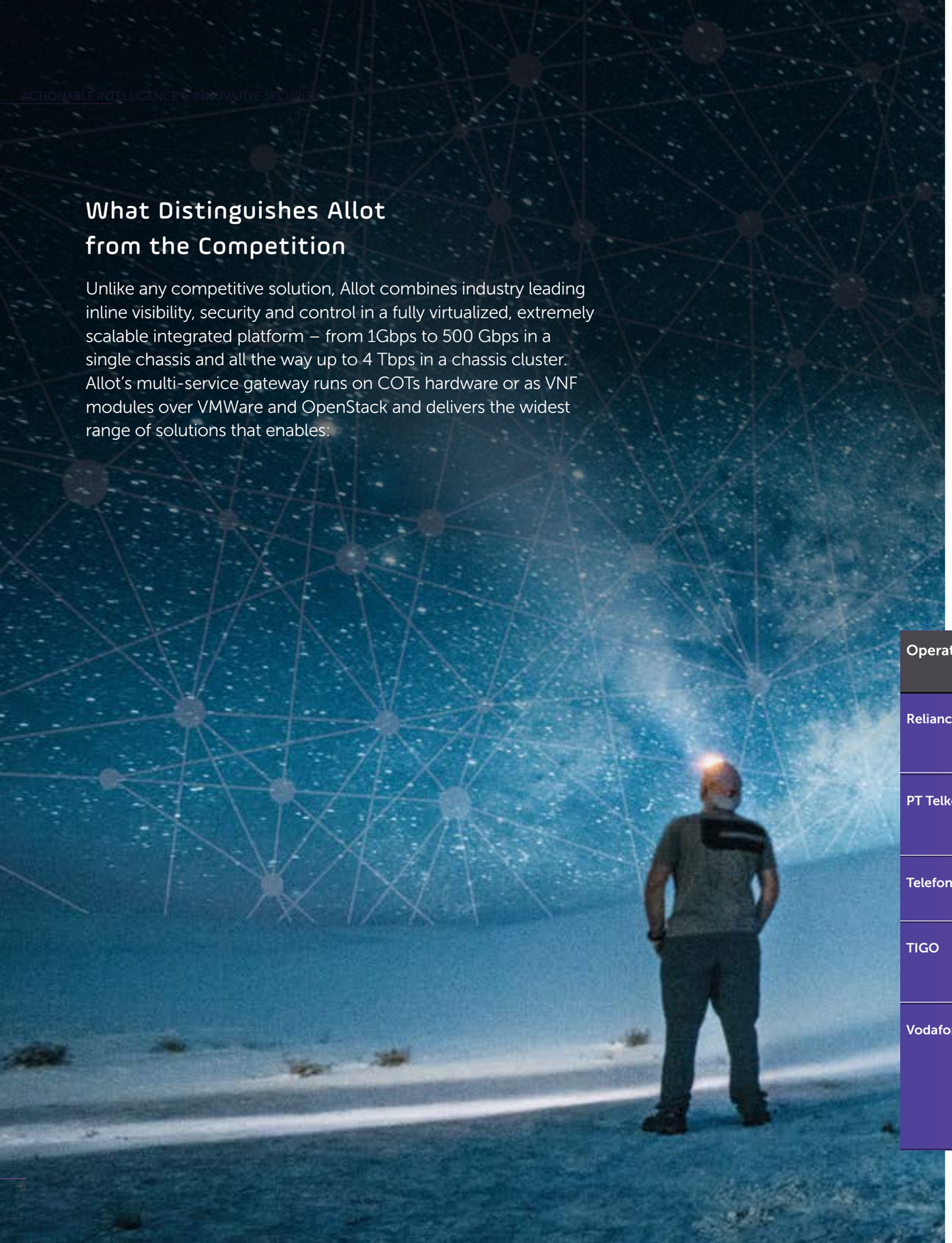
Monetizing Enterprise Customers

Provide full visibility and granular control over applications, users and network utilization. Ensure networks meet business priorities & protect against diverse threats.

Regulatory Compliance

Gives granular, big data visibility & retention of network, user and application behavior. Blocks illegal content and applications

Protects network infrastructure.



What Distinguishes Allot from the Competition

Unlike any competitive solution, Allot combines industry leading inline visibility, security and control in a fully virtualized, extremely scalable integrated platform – from 1Gbps to 500 Gbps in a single chassis and all the way up to 4 Tbps in a chassis cluster. Allot's multi-service gateway runs on COTs hardware or as VNF modules over VMWare and OpenStack and delivers the widest range of solutions that enables:

See

- Capture and curation of granular network, application, user and device data
- Customizable real-time monitoring and long-term analytics
- Data retention and export for big data and regulatory compliance

Control

- QoE-based congestion management
- Traffic management, steering and service chaining
- Policy & Charging Control of innovative service plans

Secure

- Network-based mobile & home security with threat protection, parental control
- Network-based IoT security that blocks, detects and isolates infected devices
- Terabit scale DDoS mitigation that blocks attacks within seconds

ALLOT DEPLOYMENT OVERVIEW

Operator	Country	Operation Type	Carrier Type	Subscribers Supported	Use Cases Deployed	Products Deployed
Reliance	India	Mobile	Tier1	120M	Traffic Management + PCC + Subs Managemnt + Analytics	Service Gateway + NX + CS + SMP
PT Telkom	Indonesia	Fix	Tier1 DSL	60M	Traffic Management + PCC + Subs Managemnt + Analytics	Service Gateway + NX + CS + SMP
Telefonica	Global	Mobile & Fixed	Tier1 FMC	40M	Steering + Anti Malware+ Parental Control	Service Gateway + SECaaS
TIGO	Latin America	Mobile	Tier1	38M	Traffic Management + PCC + Subs Managemnt+ Analytics	Service Gateway + NX + CS + SMP
Vodafone	Global	Fixed & Mobile	Tier1 FMC	150M	Traffic Management + PCC + Analytics export to BI + Steering to Video /Web optimization + DDoS + Security as a service with Anti Malware and Parental Controls.	Service Gateway + SECaaS

MONETIZING SECURITY AS A SERVICE TO THE MASS MARKET

NetworkSecure is the Allot Secure product that enables CSPs to provide safety and protection to their mass market customers' mobile devices. It includes built-in tools for rapid rollout of security services as well as service-awareness features that strengthen customer satisfaction and loyalty. The NetworkSecure services are delivered automatically via the network, with no need for end user device installations or updates. The two main use cases are Threat Protection and Parental Control. NetworkSecure supports both opt-in and opt-out models and includes built-in **mass-market notification and activation**, so that initial participation is very high. Opt-in or opt-out messages are easily broadcast and responses are simple and processed automatically. Once on-board, users enjoy a highly personalized experience. Icon injection enables easy access to individually personalized profiles and settings as well as personal security updates and reports. These features drive high engagement and have delivered exceptional levels of customer satisfaction.

> Allot's Network Secure allows us to deliver a more personalized and secure digital experience to subscribers."
>
> Ran Guron,
> Chief Executive Officer,
> Pelephone

Use Case	Unique Feature	Benefits
Threat Protection & Parental Control	Network Based	o Service can be activated for millions of subscribers in a very short time. o No need to download or update applications on the handsets o Simple – not dependent on OS
	Service Awareness using overlay icon and landing pages	o Users are kept aware of the value they get. o Lowers churn and raises satisfaction (NPS) o Differentiates and strengthens CSP brand
	Multi-tenancy – management per user	o Enables CSP to meet specific subscriber needs by customizing the service. o Supports a variety of profiles for Threat Protection and Parental Control
	Scale	o Any number of customers; any type of OS; designed and built for mass consumer market o Uphold the user experience when scaling out o Low cost of ownership for the CSP
Threat Protection	Rich feature list; supported by several AV engines (Kaspersky; McAfee; Bit-defender; Sophos)	o High coverage; tested to comply to different regulators and regions
Parental Control	Portal that simplifies log-in and category management	o No need for different applications on different handsets

BOTTOM LINE

Easily generates recurring revenue of 1-2 euro per month, per subscriber

ACTIONABLE INTELLIGENCE TO ENSURE QUALITY OF EXPERIENCE (QOE)

In today's competitive environment, it is critical to maintain customer satisfaction through high QoE, even under high usage conditions. Allot's SmartVisibility and SmartTraffic QoE solutions extract actionable intelligence from network, application and user behavior to enable service providers to prioritize service quality and ensure end user QoE.

Our visibility into Layers 4 through 7 traffic, including the ability to identify encrypted applications, enables automatic, policy-driven bandwidth shaping that minimizes congestion and ensures the best possible QoE according to your priorities. In addition, along with SmartPCC, this visibility enables CSPs to deliver innovative service plans, monitor data usage, and enforce policy across any network.

Actionable Intelligence also drives the ability to detect zero-day exploits during volumetric DDoS attacks, as described in the following section. It is also at work in the detection of fraudulent usage behavior as well as identification of high-risk pre-churn behavior patterns among dissatisfied users.

BENEFITS

- Save at least 10% of access bandwidth costs
- Defer capacity expansion by 1-2 years
- Lower OPEX through automation
- Reduce revenue leakage by 15%

USE CASE

At a large mobile operator, we demonstrated the ability to automatically:

- Reduce congested cells by 25% during peak hours
  - Overall reduction of heavily congested cells (PRB > 90%) by 25% over the day
  - Overall reduction of congested cells by 10% over the day
- Increase number of connected users by 5% during peak hours
- Improve browsing experience via 25% increase of average throughput
- Reduce Internal RTT across all applications

DDOS MITIGATION AND BOT CONTAINMENT

DDoS (Distributed Denial of Service) attacks pose some of the most serious threats to your network, your services, your customers and your business. With the growth of IoT, that threat has increased as botnets created by hundreds of thousands of infected devices can disable services for millions of users. Every second counts when you're under attack. And so does maintaining your Quality of Service.

Allot DDoS Secure is a DDoS Protection and Threat Containment solution designed to mitigate large scale DDoS attacks in real-time and isolate possible threats originating from individual end-points/subscribers that disrupt the performance and integrity of network infrastructure and services. Allot's Real-time DDoS Mitigation is the only solution that:

- Thwarts both inbound and outbound attacks inline, within seconds, before they can disrupt your network service.
- Monitors 100% of network traffic to accurately foil attacks of any volume without impacting innocent bystanders.
- Uses machine learning and artificial intelligence to automatically detect even unknown attacks.
- Combines DDoS mitigation with DPI-based traffic management to preserve legitimate traffic and maintain your service quality under the most severe conditions.
- Offers unrivalled scalability so you can mitigate even large terabit attacks from multiple vectors.

Incoming network level DDoS attacks are identified using Network Behavior Anomaly Detection (NBAD) technology. Outbound host abusive behavior attacks from IoT botnets, spambots or other devices connected to your network, are identified using Host Behavior Anomaly Detection (HBAD) technology. In both situations, deviations from normal behavior are used to identify attack scenarios in real-time.

> "Allot DDoS Protection and Bot Containment services enabled immediate and effective IoT DDoS defense without installing new equipment or altering existing security systems."
>
> Tier 1 Service Provider, LATAM

IOT: ENTERPRISE AND SMART HOME SECURITY

The Internet of Things (IoT) has proven to be notoriously insecure and security concerns are the number one reason that many enterprises avoid making IoT a significant part of their business operations. Allot's IoTSecure solution presents service providers with a huge opportunity to further monetize their enterprise connectivity services.

Allot's IoTSecure solution delivers proven carrier-class security, behavior analysis, and traffic intelligence and control. It enables your customers to configure the following services through a customer management portal.

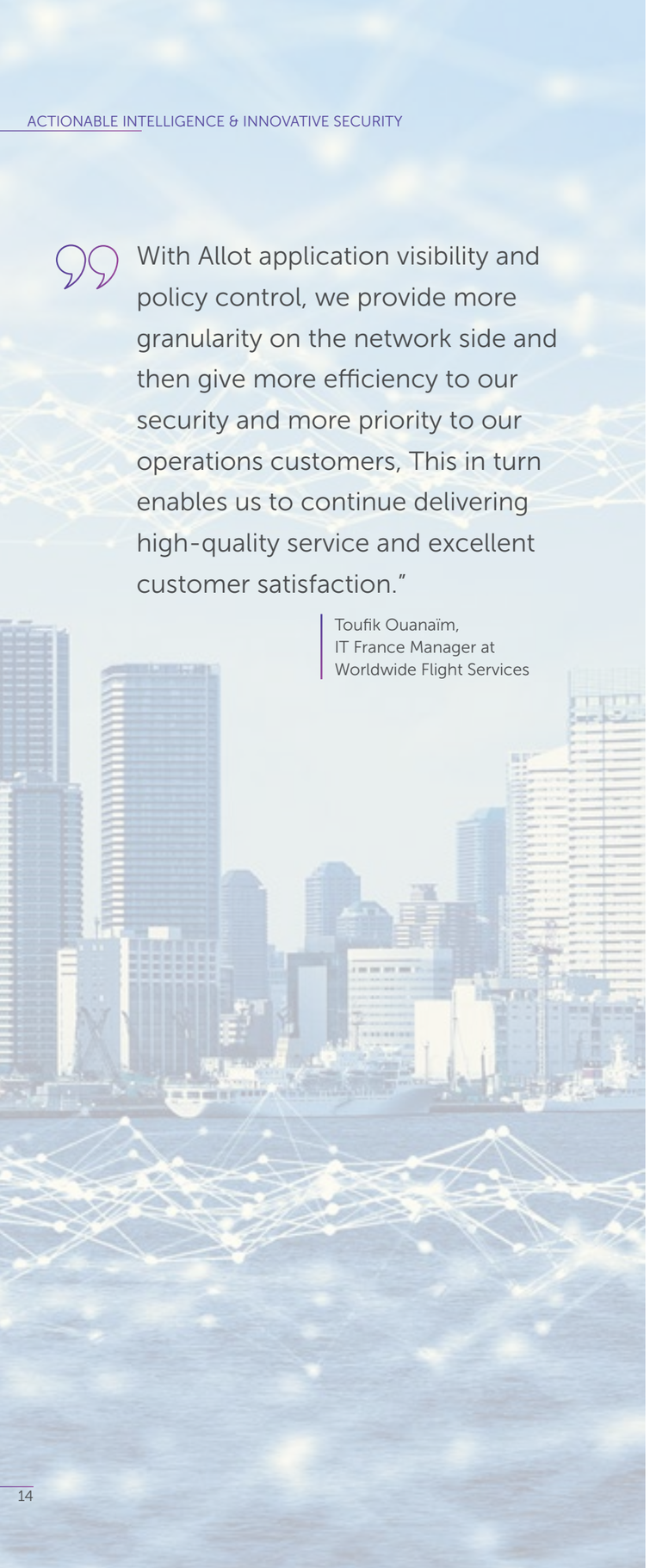
- **Behavior Assurance**: The ability to define policies that manage IoT deployments
- **Behavior Profiling**: An artificial intelligence approach to IoT analytics for detecting compromised IoT devices and to assist in troubleshooting and planning.
- **IoT Security**: A network-based security solution that protects against malware and botnets and allows remote remediation of suspect devices

IoTSecure delivers the following benefits to service providers:

- **Service differentiator:** Introduces security as a differentiating competitive advantage.
- **Revenue generator:** Drives an additional 10-15% revenue on top of connectivity charges.
- **Use case agnostic:** Applicable to any IoT service and is aligned with CSP core business.

Our HomeSecure solution offers your subscribers a single, out-of-the-box security service that removes the complexity of securing devices in the home and increases your connectivity revenue by 10-15%.
By remotely installing the HomeSecure thin client on subscribers' home CPEs, you will be able to centrally manage all the security for their connected devices. And your users will also receive an app that keeps them engaged with their connected home security.
The Allot HomeSecure agent applies three layers of security that:

- **Protect devices against external threats:** based on machine learned behavior profiles
- **Secure the local network:** by blocking lateral propagation of infections
- **Harden the CPE:** to prevent the CPE itself from being compromised



> With Allot application visibility and policy control, we provide more granularity on the network side and then give more efficiency to our security and more priority to our operations customers, This in turn enables us to continue delivering high-quality service and excellent customer satisfaction."
>
> Toufik Ouanaïm,
> IT France Manager at
> Worldwide Flight Services

MONETIZING ENTERPRISE CUSTOMERS

In addition to helping you deliver optimal subscriber QoE, Allot also enables enhanced monetization of enterprise customer. The Allot Secure Service Gateway (SSG) will help your enterprise customers increase their productivity and protect their operations. By delivering full visibility and granular control over applications, users and network utilization, the SSG enables removal of risky applications, control of recreational traffic and, most importantly, ensures that your enterprise customers' networks meet their business priorities. In addition, you can reduce the total cost of ownership of your security investment by leveraging both the built-in Secure Web Gateway function that protects your users against diverse web threats (such as Ransomware, Denial of Service attacks and Bot infection) and behavioral engines that mitigate DDoS attacks and combat botnets. At thousands of enterprises around the world we have demonstrated high-value use cases, such as:Allot's IoTSecure solution delivers proven carrier-class security, behavior analysis, and traffic intelligence and control. It enables your customers to configure the following services through a customer management portal.

- Understand how network resources are consumed before making infrastructure investments
- Define real-time traffic management policies that align performance to business priorities and adjusts IP traffic flows dynamically when links are congested
- Define tiered traffic management policies based on individual levels of service for specific user profiles
- Reduce the enterprise attack surface and increase productivity by identifying and blocking risky applications such as anonymizers and peer-to-peer applications
- Maintain maximum QoE for all legitimate traffic by blocking threats and shaping traffic

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 online 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.

BENEFITS

Allot's SmartSentinel offers a unique, unified solution based on massively scalable, in-line protection that inspects every packet and delivers the following key benefits:

- Granular, big data visibility into network, user and application behavior
- Blocking illegal content, such as pornography, violence, drugs, child abuse, fake and untruthful content and illegal applications
- Unlimited retention of detailed usage records
- Protection of network infrastructure against DDoS attacks

USE CASE

Government regulations required the following functions:

- URL filtering based on a government database
- Subscriber logging & record storage
- Search & reporting tool to access stored record
- VPN Blocking to prevent anonymous online activity

ALLOT ADVANTAGES vs. COMPETITION

DPI

Not just DPI - a highly scalable VAS Gateway that helps CSPs *monetize* their network:

- Allot Security VAS
- Flexible steering to other VAS devices

- Just a DPI
- No Security Value added Services
- Limited steering, no chaining

Security Offering

Unique Security Offering

- **NetworkSecure**: Millions of dollars in revenues, >20M subscribers protected
- **DDoS Secure**: Powerful, bidirectional solution with over 70 deployments

- No network-based security offer
- DDoS is barely deployed, inbound only legacy system

Time-to-Market

Time-to-Market Accelerator – Lower TCONetworkSecure:

- **Easy GUI to set policies & launch services without expensive Professional Services**
- Much higher port density. Much lower impact from added functionality

- Configuration is complex requiring professional services that double cost of project
- Low scalability, performance suffers as functionality is added

Future Proof

- Advanced NFV compliance – assures Next Gen architecture and throughput
- Clear, committed roadmap protects customer investments

- Virtualization limited to COTS support
- Roadmap is not clear

Allot's comprehensive solutions:

...The result is a differentiated service that increases customer loyalty and ARPU.

LATAM Global CSP

July 2019

www.allot.com