

Use Cases

Communications Service Providers



CONTENTS

INTRODUCTION	5
USE CASES BY SOLUTION DOMAIN	
NETWORK VISIBILITY	6
Customer Segmentation	7
Optimize Customer Care	8
Identify Potential Churners	9
Technology Version Awareness	11
Network Resource Planning	12
Customer QoE	13
Prepaid Behavior Analysis	14
Revenue Impact Analysis and Fraud Detection	15
Security Analysis	16
Service Plan Evaluation	17
POLICY & CHARGING CONTROL	18
Application-based Charging	19
HTTP Header Enrichment	20
OTT Content Bundling	21
OTT Premium Content	23
Service Tiering	24
Tethering Detection	25
Turbo Boost	26
Volume-based Charging	27
TRAFFIC MANAGEMENT	28
QoE-based Congestion Management	29
Layer 7 Steering for VAS Integration	31
Fair Use Management	32
Multi-tenant Solution for Visibility & Control for Enterprise Customers	33
OTT Video Optimization	34
Autonomous Systems-BGP Awareness	35
SECURITY VAS	36
Security as a Service	37
Subscriber Engagement for Security VAS	38
Unified Security	39
Securing the SmartHome	40
Parental Control	41
DDoS PROTECTION	42
Bidirectional DDoS Prevention	43
DDoS Security as a Service for Enterprise	44
DDoS Security as a Service for Interconnect Carriers	45

IOT SECURITY	46
IoT Security as a Service	47
Improve IoT operational efficiency	48
Protect infrastructure from IoT borne attacks	49
REGULATORY COMPLIANCE	50
Anti-spam (Blacklist Prevention)	51
Blacklist URL Filtering	52
Unified Regulatory Compliance	53
Usage Records Store & Retrieve	54
Bill Shock Prevention	55

INTRODUCTION

Allot Communications is a leading global provider of innovative network intelligence and security solutions for service providers, helping you deliver enhanced value to your customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, and network-based security services. Your customers demand secure and innovative services at a high Quality of Experience - we help you meet and exceed their demands.

When visibility is clear and network intelligence is accurate, you can make smarter, real-time decisions to truly manage your network, engage your customers and innovate with new service offerings. We give you the tools to optimize and capitalize on every opportunity; to learn about users and network behaviors; to improve quality of service and reduce costs; and to protect your networks and your users from malicious attacks.

All of this is achieved while deploying new services more quickly than ever before to bring increased value to your customers.

The choice may seem simple, but the path is complex. An experienced, knowledgeable, and innovative partner can make all the difference in meeting customer expectations.

Allot Communications is your partner for high quality and secure network services.

The use cases in this booklet present some of the many ways in which Allot works with leading service providers to efficiently manage their network and deploy innovative and secure services and reap the rewards.

The Service Provider Use Cases are organized into the following seven solution domains:

- Network Visibility
- Policy and Charging Control
- Traffic Management
- Security VAS
- DDoS Protection
- IoT Security
- Regulatory Compliance

NETWORK VISIBILITY

When you truly know what’s happening on your network, you can make better business decisions. Allot gives you complete visibility of all application and user traffic in granular detail with Allot SmartVisibility, which is viewed through built-in dashboards or custom reports that you create on demand. Optional export of rich data records enhances the insight you gain from external BI and big data systems.

Key Benefits

- Gain deeper understanding of customer online activity and preferences
- Increase ARPU through better targeting of services/promotions
- Reduce churn with “stickier” services

Identify subscriber interests and usage patterns

- Analyze data usage patterns of subscribers, applications, and devices
- Segment subscribers based on areas of interest and usage patterns
- Target promotions and opt-in adverts tailored to each segment
- Leverage segmentation profiles to attract advertisers and other revenue opportunities

Powered by Allot Service Gateway

- NetXplorer
- ClearSee
- Subscriber Management Platform

Departments

Marketing/Engineering/
Operations/Security

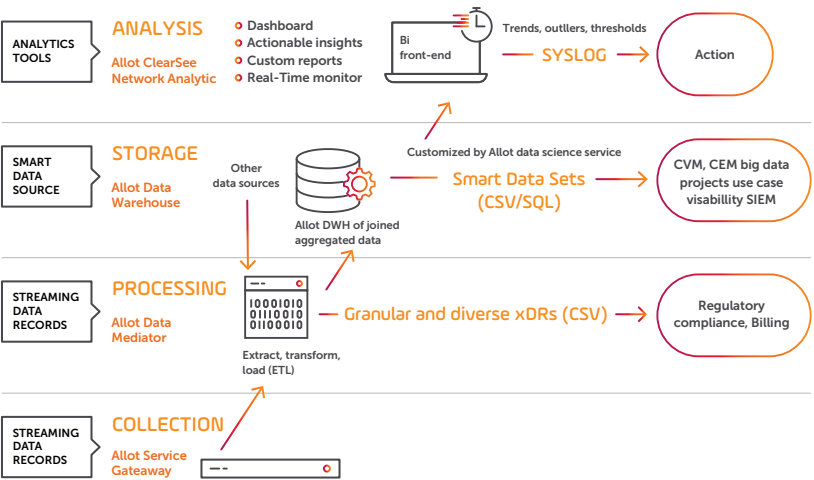
Technology

Fixed, Mobile, Converged

NETWORK VISIBILITY CUSTOMER SEGMENTATION

The ability to identify subscriber interests and usage patterns enables service providers to introduce targeted promotions and to benefit from other revenue generating opportunities. For example, one user segment may be characterized as having an interest in gadgets, while the subscribers in another segment are music lovers. By identifying these interest segments - along with other attributes such as usage patterns and type of device – the operator can launch effective promotions that offer subscribers relevant products and services such as new or additional devices or personalized service plans. Subscriber segmentation also offers abundant opportunities for revenue generation from advertising.

GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC

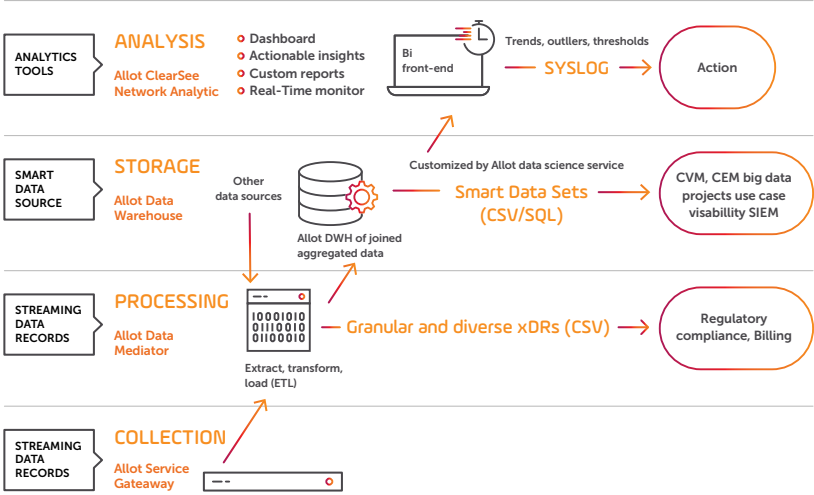


NETWORK VISIBILITY

OPTIMIZE CUSTOMER CARE

Every interaction with your customer is critical. The right kind of usage and activity analytics can assist Customer Care personnel in resolving customer issues. For example, customers may complain that their handset battery requires frequent recharging and is running out of juice after only a few hours of use. While the usual suspect may be the battery, the customer’s usage history points to a recent download of one or more bandwidth-intensive applications as well as frequent use of that application. The history may also show that the downloaded application works better with a later version of the device’s operating system. Armed with this usage history and analysis, support personnel could recommend using an alternative application that is easier on the battery, upgrading the device OS, or upgrading the battery, or all three options. With so many factors affecting data service, customers value a service provider who is knowledgeable and can resolve problems quickly.

GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC



Key Benefits

- Reduce trial and error in resolving customer complaints
- Improve your Customer Care service
- Enhance your brand image

Customer Care Optimization in Action

- Customer contacts Call Center with complaint
- Call Center rep consults customer profile and recent activity
- Profile analysis assists in pinpointing the problem
- Call Center resolves the problem faster and better

Powered by Allot Service Gateway

- NetXplorer
- ClearSee
- Subscriber Management Platform

Departments

Marketing/Engineering/Operations/Security

Technology

Fixed, Mobile, Converged

Key Benefits

- Reduce trial and error in resolving customer complaints
- Improve your Customer Care service
- Enhance your brand image

Identify Potential Churners in Action

- Customer contacts Call Center with complaint
- Call Center rep consults customer profile and recent activity
- Profile analysis assists in pinpointing the problem
- Call Center resolves the problem faster and better

Powered by Allot Service Gateway

- NetXplorer
- ClearSee
- Subscriber Management Platform

Departments

Marketing/Engineering/Operations/Security

Technology

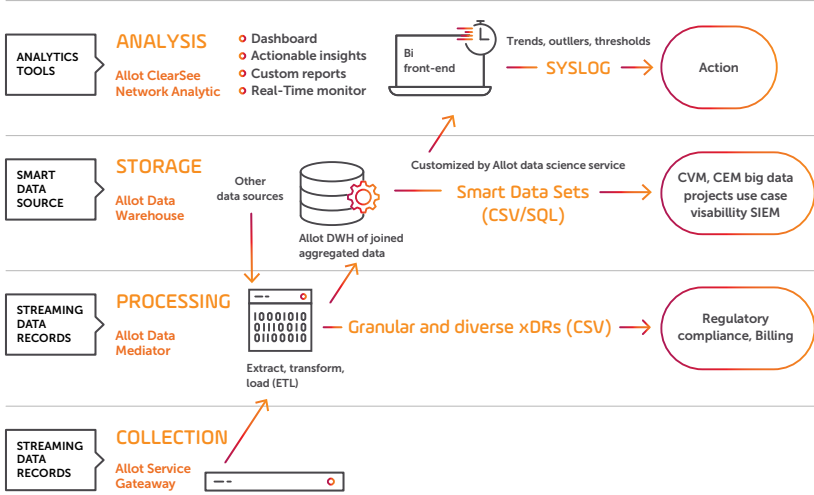
Mobile, Converged

NETWORK VISIBILITY

IDENTIFY POTENTIAL CHURNERS

It is estimated that it costs 7 times as much to win new customers as to keep existing ones. Using advanced analytics capabilities, it is possible to craft reports that identify high risk churners based on a combination of activities such as reduced activity, visits to competitor sites and poor QoE. One can then reach out to such customers with attractive, personalized offers and care to win back their loyalty

GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC



Key Benefits

- Understand technology utilization trends
- Plan for new technology
- Migrate on time/on budget

Technology Version Awareness in Action

- Analyze trends in technology utilization
- Create well-founded migration plan
- Implement efficiently

Powered by Allot Service Gateway

- NetXplorer
- ClearSee
- Subscriber Management Platform

Departments

Marketing/Engineering/
Operations/Security

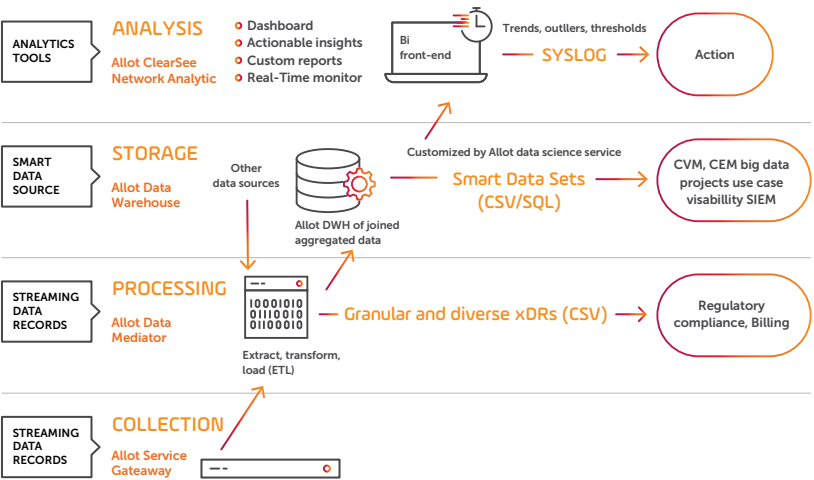
Technology

Fixed, Mobile, Converged

NETWORK VISIBILITY TECHNOLOGY VERSION AWARENESS

Keeping up with new technologies can be quite costly. With constant pressure to stay ahead of changes, service providers may be tempted to overspend early in the curve - earlier than they need to. By gaining clear visibility into actual usage trends within their customer base, they can plan "just in time" migrations and keep CAPEX and OPEX as low as possible

GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC

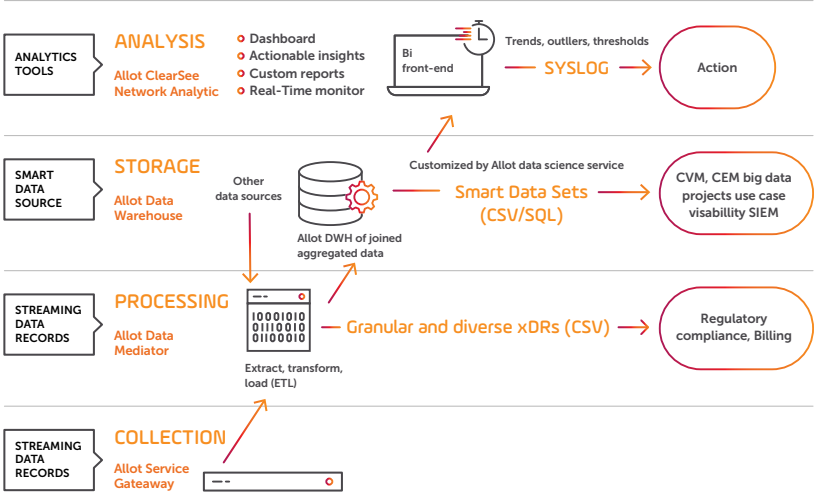


NETWORK VISIBILITY

NETWORK RESOURCE PLANNING

Network planning relies on accurate and meaningful information regarding congestion episodes on the network, why they occur, and their effect on subscriber Quality of Experience (QoE).. For example, real-time analytics can show which subscribers, applications and devices are consuming the bandwidth in a temporarily congested cell, while historical analysis can be used to identify the usage patterns that make a cell chronically congested. The effects of congestion may be felt keenly by video consumers who experience more stalls, stutters and long load times. Analyzing QoE per subscriber, application and device in congested cells can help operators identify problem areas and better plan around them. For example, expedited forwarding and video optimization may alleviate most of the QoE problems, rather than bandwidth expansion.

GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC

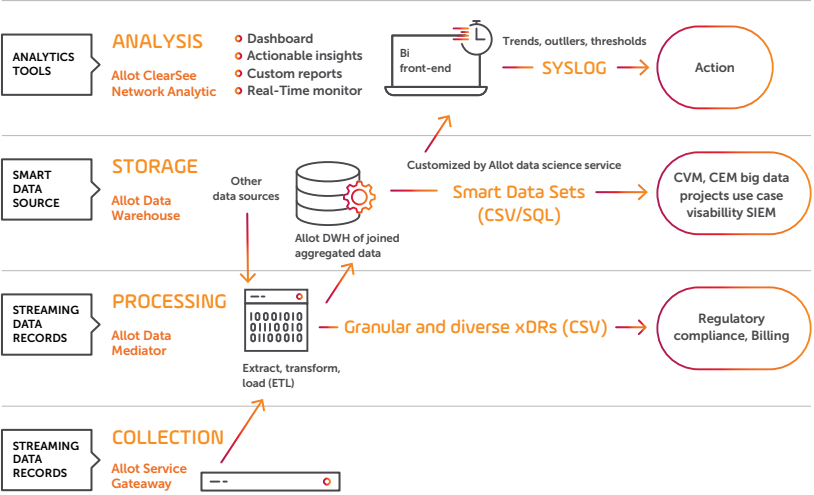


NETWORK VISIBILITY

CUSTOMER QoE

To ensure high customer QoE, one must measure and understand in detail the factors that influence performance issues related to browsing and video consumption. By analyzing in detail where, when and why congestion is impacting user experience, service providers can optimize network expansion to exactly fit current and projected needs—avoiding unnecessary spending, saving both CAPEX and OPEX.

GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC

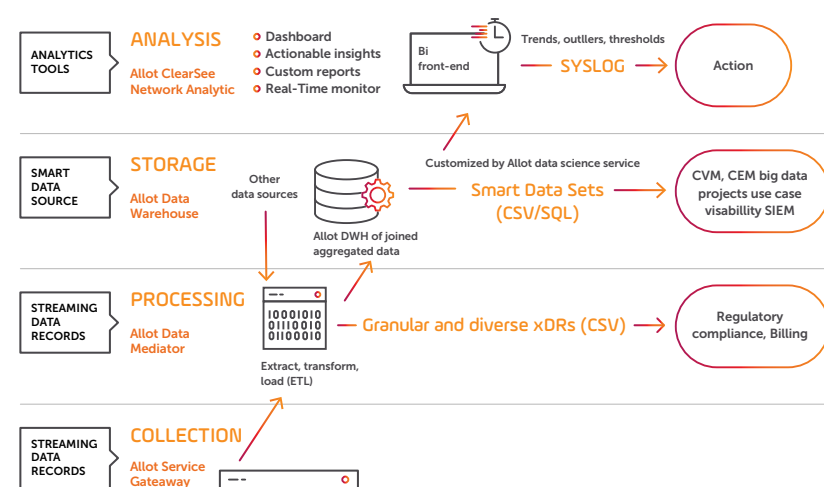


NETWORK VISIBILITY

PREPAID BEHAVIOR ANALYSIS

Prepaid customers comprise a significant segment of users in mobile data networks. However, their activity and preferences are mostly unknown. This limited relationship makes it easier for them to churn. Prepaid Behavior Analysis allows service providers to change the nature of the relationship by providing valuable insight into the online activity of prepaid customers. Usage trends regarding popular applications, time-of-day patterns, device, and other parameters help service providers identify different profiles within the prepaid community so they can target the right kind of value to this important segment. For example, behavior analysis can be used to incentivize users of bandwidth-intensive applications to increase the amount of their regular top-up, or move up to a higher-tier prepaid package. It can also assist in targeting relevant ad campaigns to prepaid customers.

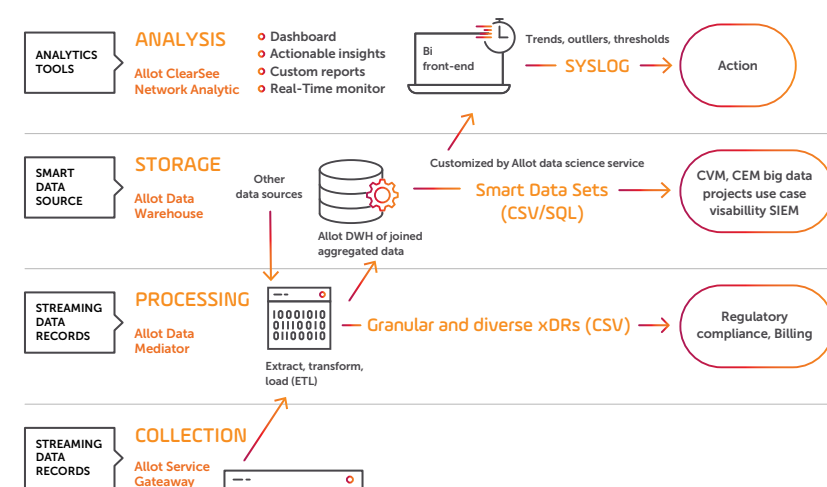
GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC



NETWORK VISIBILITY
REVENUE IMPACT ANALYSIS AND
FRAUD DETECTION

It has been estimated that service providers lose 10-20% of potential revenue to fraudulent activity that bypasses usage quotas and avoids payment for data consumption. This clearly impacts the bottom line and may also contribute to congestion and unnecessary network expansion if unchecked. By identifying these activities and taking steps to block them, service providers can ensure they are properly compensated for all network usage.

GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC



Key Benefits

- Elevate your relationship with prepaid customers
- Reduce the risk of prepaid churn
- Increase opportunities for revenue generation

Prepaid Behavior Analysis in Action

- Track prepaid usage per application, volume, and device
- Combine usage data with location, point of sale, and other known parameters
- Analyze prepaid behavior and segment accordingly
- Prepaid Behavior Analysis in Action Target prepaid segments with more appealing packages

Powered by
Allot Service Gateway

- NetXplorer
- ClearSee
- Subscriber Management Platform

Departments

Marketing/Engineering/
Operations/Security

Technology

Mobile, Converged

Key Benefits

- Identify fraudulent activity
- Close security loopholes
- Assure revenue per usage

Revenue Impact Analysis and Fraud Detection in Action

- Establish baseline application behavior
- Monitor and detect anomalous behavior patterns
- Alert service providers to implement mitigation

Powered by
Allot Service Gateway

- NetXplorer
- ClearSee
- Subscriber Management Platform

Departments

Marketing/Engineering/
Operations/Security

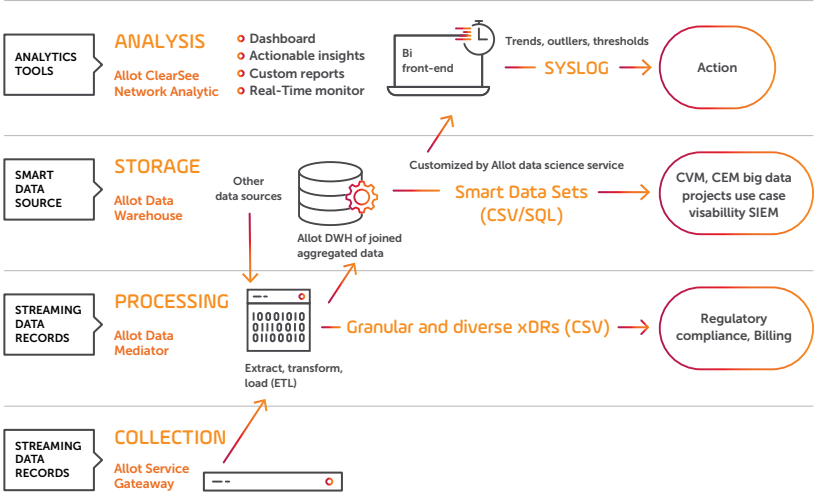
Technology

Fixed, Mobile, Converged

NETWORK VISIBILITY SECURITY ANALYSIS

Studies indicate that many mass market subscribers want their service provider to solve their connectivity security issues on their behalf. By correlating users who have experienced security issues with demographics of customers that pay for security Value Added Services, SPs can target specific value-added security services to likely candidate customers

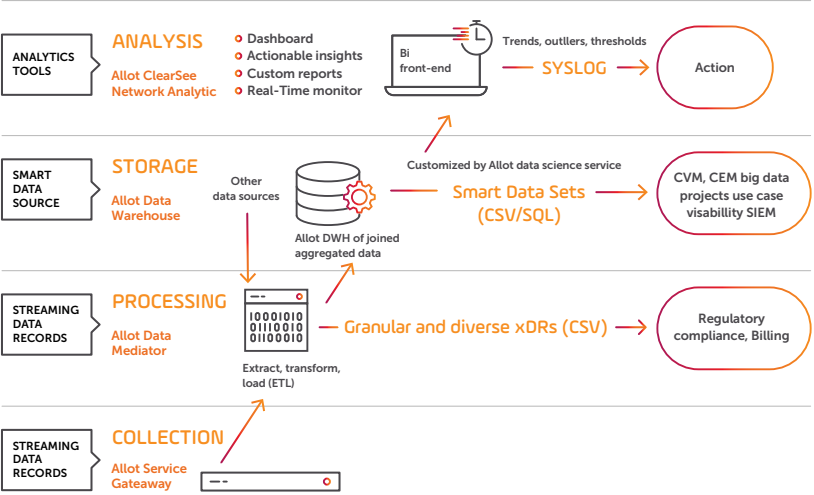
GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC



NETWORK VISIBILITY SERVICE PLAN EVALUATION

Tiered plans and service bundles do not always get utilized as expected by operators. Granular visibility into correlation between user demographics, device types and package utilization enable the service provider to fine-tune offerings to match customer segments, thereby increasing network usage and customer ARPU.

GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC



POLICY CONTROL & CHARGING (PCC)

Maximize customer lifetime value by leveraging application-based and usage-based data plans that cater to the unique and dynamic needs of prepaid, postpaid, business, and IoT customers. Allot's Smart PCC solutions integrate seamlessly with authentication, provisioning and charging systems to assure fast service roll-out and time-to-revenue.

Key Benefits

- Increase ARPU
- Enhance customer choice and increase loyalty
- Differentiate your service offering

Application-based Charging in Action

- Customer opts-in to "Social Mingler" plan
- Plan based on data cap with unlimited use of social networking apps
- Exclude Facebook, Twitter, WhatsApp, Instagram, LinkedIn from data cap
- Send monthly usage report in customer bill indicating "free" data volume used

Powered by Allot Service Gateway

- NetXplorer
- ClearSee
- Subscriber Management Platform

Departments

Marketing/Engineering/
Operations/Security

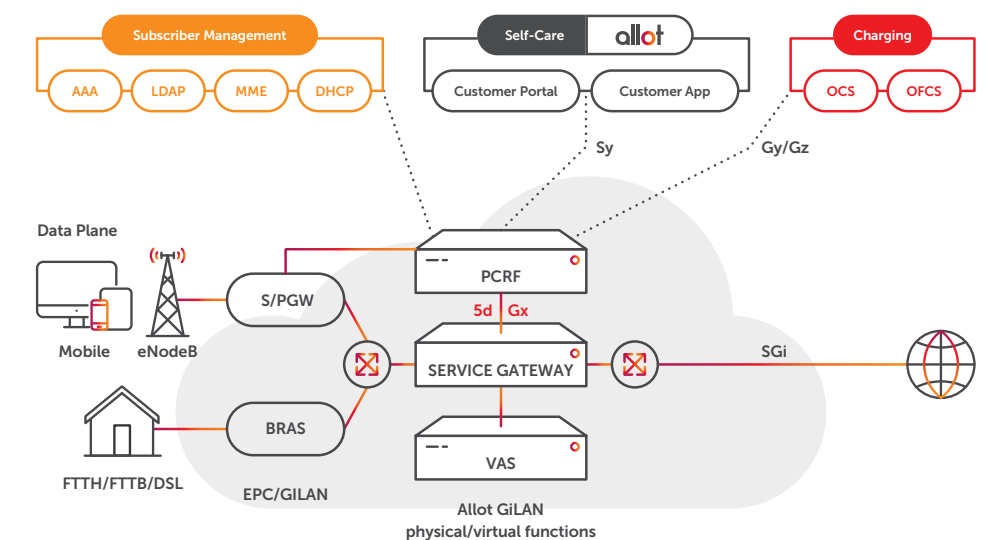
Technology

Mobile, Converged

POLICY CONTROL & CHARGING APPLICATION-BASED CHARGING

The ability to identify applications at Layer-7 allows operators to differentiate their offering with a range of unique service plans based on gaming, social networking, streaming video, basic email, and other popular applications. For example, operators may identify many customers who are "Social Minglers" meaning they are heavy users of social networks. This segment can be offered zero-rating on popular social networking apps so that usage is not counted against their data cap. Similarly, frequent gamers would be attracted to a plan that offers guaranteed quality of service for World of Warcraft, Call of Duty, and other interactive games.

DIFFERENTIATED OFFERINGS AND PERSONALIZED CUSTOMER EXPERIENCE



POLICY CONTROL & CHARGING

HTTP HEADER ENRICHMENT

Service providers seek ways to leverage customer information to improve and personalize their online experiences. By forwarding anonymized customer information to OTT and Content provider web sites, these partners can in turn provide personalized responses/content that improves the end user experience, driving improved business models for the Service Provider.

Key Benefits

- Increase ARPU
- Improve User Experience/ increase loyalty
- Strengthen OTT partnerships

HTTP Header Enrichment in Action

- Offer personalized services
- Partner with OTT and Content Providers
- Enrich HTTP headers of customer requests
- Deliver personalized services

Powered by Allot Service Gateway

- NetXplorer
- Subscriber Management Platform

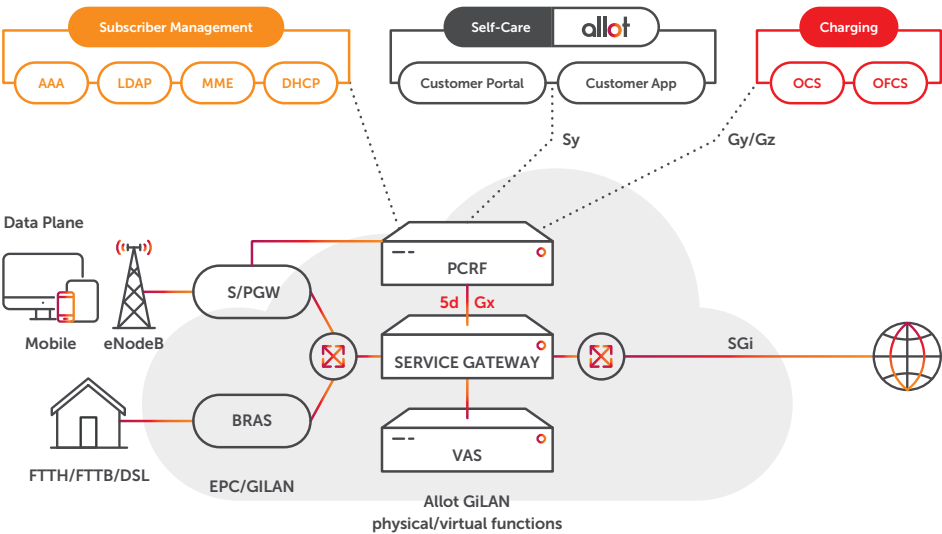
Departments

Marketing/Operations

Technology

Mobile, Converged

DIFFERENTIATED OFFERINGS AND PERSONALIZED CUSTOMER EXPERIENCE



POLICY CONTROL & CHARGING

OTT CONTENT BUNDLING

Over-the-top content is an integral part of the digital lifestyle. One of the ways service providers can capitalize on this phenomenon is by generating and sharing revenue through tiered bundles of popular OTT content and services. For example, service providers can partner with local content providers to bundle their music, games, movies, video, and social networking applications into a variety of tiered packages aimed at different customer segments. Bundled applications may be loaded onto smartphones at the point of sale, together with usage caps, overage policy, and unified billing by the service provider for pay-for-use content.

The bundle may include content caching or video optimization to ensure great QoE. It may also offer options for targeted advertising based on in-depth analysis of subscriber behavior and bundle popularity. With so many kinds of local and global content coming online all the time, service providers have unlimited opportunity to launch new business ventures with OTT providers and share the revenue.

Key Benefits

- Create new sources of revenue together with OTT content providers
- Differentiate your service offering
- Reduce churn

HTTP Header Enrichment in Action

- Service bundles with various combinations of OTT content/services
- Provision QoS, volume cap, and charging rules for each bundle
- Track and share usage statistics for targeted advertising
- Provide unified billing for all services

Powered by Allot Service Gateway

- NetXplorer
- Subscriber Management Platform

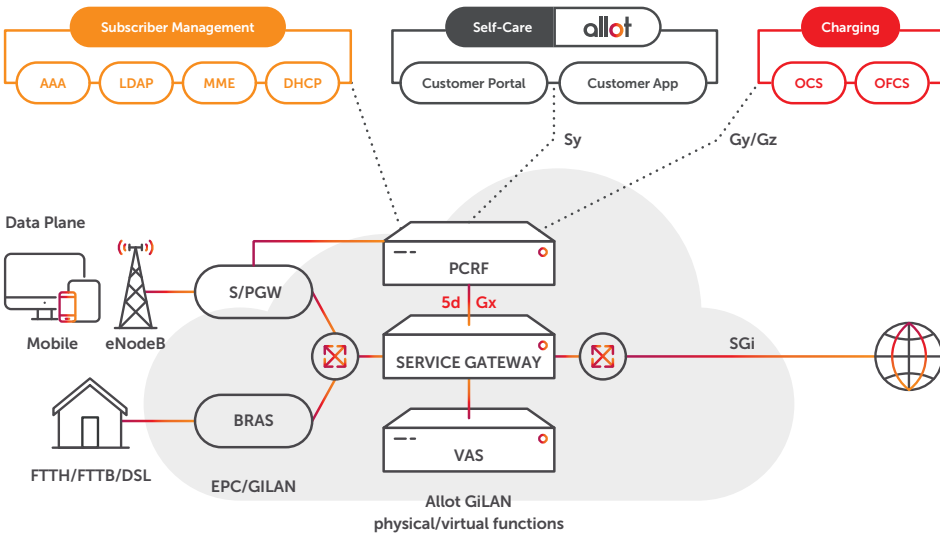
Departments

Marketing/Operations

Technology

Mobile, Converged

DIFFERENTIATED OFFERINGS AND PERSONALIZED CUSTOMER EXPERIENCE



Key Benefits

- Differentiate your offering to high-end customers
- Expand revenue-share business
- Increase ARPU

HTTP Header Enrichment in Action

- Create tiered packages for delivery and charging of premium OTT content/services
- Share revenue with OTT providers from new customer acquisitions
- Track and share usage statistics for targeted advertising
- Provide unified billing for all services

Powered by Allot Service Gateway

- NetXplorer
- Subscriber Management Platform

Departments

Marketing/Operations

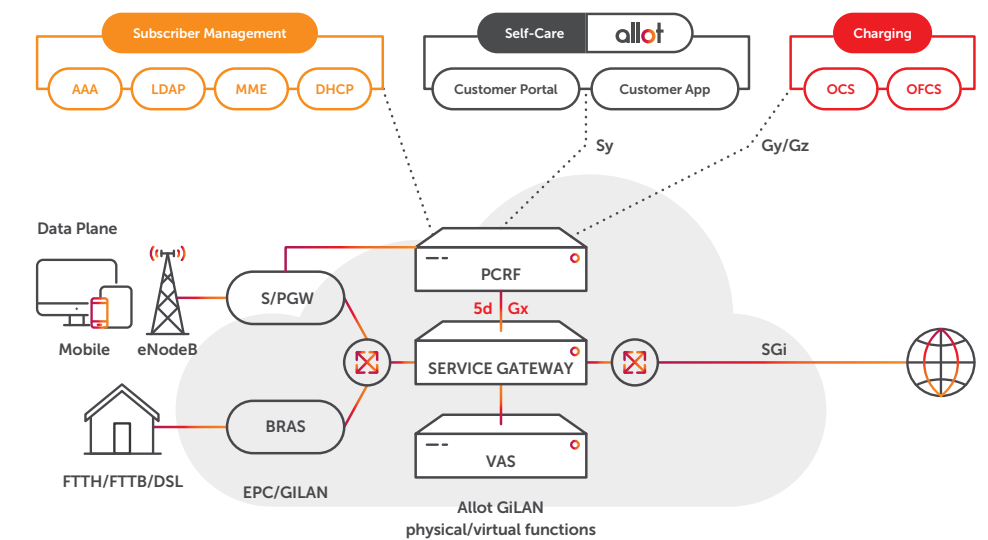
Technology

Mobile, Converged

POLICY CONTROL & CHARGING OTT PREMIUM CONTENT

While most over-the-top content is free, many content providers also offer premium Internet content and services for a fee. Service providers can capitalize on this growing phenomenon by leveraging their unique ability to enable access, shape the user experience and to track and analyze OTT usage. For example, service providers can help popular music-, video-, or TV-on-demand providers to expand their pay-for-use business by bundling the OTT service together with smartphone acquisition, high-speed access, guaranteed QoE, and unified billing in a premium package. The premium-content relationship may share revenue and also offer options for targeted advertising based on analysis of subscriber behavior and application usage.

DIFFERENTIATED OFFERINGS AND PERSONALIZED CUSTOMER EXPERIENCE



Data service providers use service tiering to tailor competitive service plans to specific market segments and subscriber preferences. Service plans may be tiered according to different speeds (Mbps, Gbps), QoS, usage allowances, Happy Hours, fair use provisions, application-based SLAs and more. For example, a basic tier could offer high speed but low monthly data cap, while a premium tier offers high speed, unlimited data volume, and expedited forwarding for Streaming Video and Gaming applications. Tiered plans can be rolled out for specific devices as well. In this way, operators can target each customer with the right service plan at the right price.

The diagram illustrates the Allot GiLAN physical/virtual functions architecture. It shows the integration of various network functions and their connections to the core network components.

Subscriber Management: Includes AAA, LDAP, MME, and DHCP.

Self-Care: Includes Customer Portal and Customer App.

Charging: Includes OCS and OFCS.

Data Plane: Includes Mobile (laptop and smartphone) and eNodeB (cell tower).

FTTH/FTTB/DSL: Represented by a house icon.

Core Network Components:

- S/PGW:** Connected to Mobile and eNodeB.
- BRAS:** Connected to FTTH/FTTB/DSL.
- PCRF:** Connected to S/PGW and SERVICE GATEWAY.
- SERVICE GATEWAY:** Connected to S/PGW, PCRF, and VAS.
- VAS:** Connected to SERVICE GATEWAY.
- SGi:** Connected to SERVICE GATEWAY and the Internet (globe icon).

Interfaces and Connections:

- Sy:** Connects Self-Care (Customer Portal/App) to PCRF.
- Gy/Gz:** Connects Charging (OCS/OFCS) to PCRF.
- 5d:** Connects S/PGW to SERVICE GATEWAY.
- Gx:** Connects PCRF to SERVICE GATEWAY.

Labels:

- EPC/GiLAN:** Labels for the S/PGW and BRAS components.
- Allot GiLAN physical/virtual functions:** The overall system name.

- Increase revenue and upsell opportunities
- Differentiate your service offering
- Enhance customer satisfaction

- Create policy rules for each tiered service plan
- Assign customers to the tiered plan of their choice
- Automatically enforce tier speed, QoS, data cap, etc. on subscriber traffic in real-time
- Automatically enforce tier charging rules and create charging records

- NetXplorer
- Subscriber Management Platform

Marketing/Operations

Mobile, Converged

- Increase ARPU through optional tethering plans
- Increase customer satisfaction
- Block illegal tethering

- Offer premium plans that include tethering
- Detect tethering in real-time
- Apply premium charging and block unpaid for tethering attempts

- NetXplorer
- Subscriber Management Platform

Marketing/Operations

Mobile, Converged

In many geographies, mobile broadband is the most accessible broadband option available and some customers exploit tethering to enable secondary users to ride for free on their data plans. Tethering is difficult to detect but if detected, it can be offered as an upsell and blocked when it has not been paid for.

The diagram illustrates the Allot GiLAN architecture, showing the integration of various systems and the flow of data and control plane traffic.

Subscriber Management (Orange): Includes AAA, LDAP, MME, and DHCP.

Self-Care (Dark Grey): Includes Customer Portal and Customer App.

Charging (Red): Includes OCS and OFCS.

Data Plane (Left): Includes Mobile (laptop and phone) and FTTH/FTTB/DSL (house icon).

EPC/GiLAN (Center): Includes S/PGW, BRAS, PCRF, SERVICE GATEWAY, and VAS.

Interfaces and Connections:

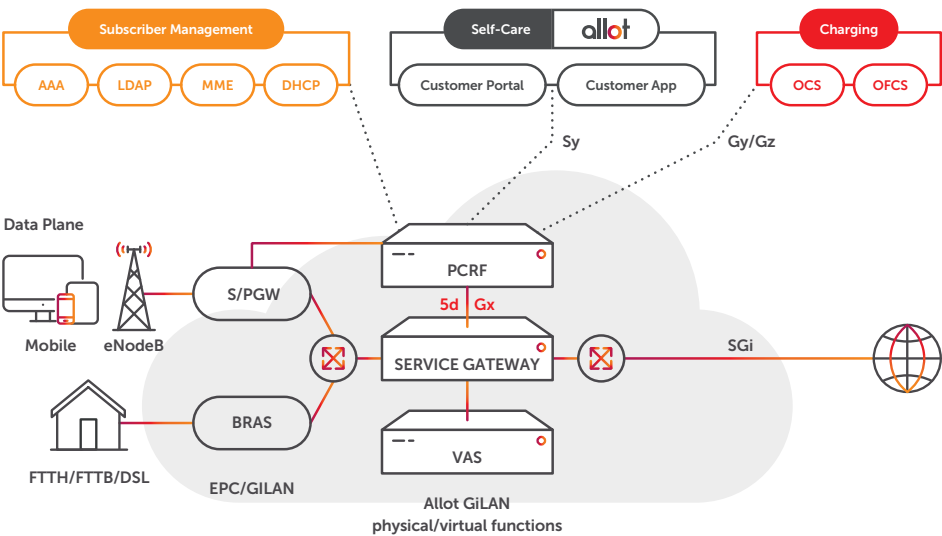
- Sy:** Connects the Self-Care systems (Customer Portal and Customer App) to the PCRF.
- Gy/Gz:** Connects the Charging systems (OCS and OFCS) to the PCRF.
- Sd:** Connects the S/PGW to the SERVICE GATEWAY.
- Gx:** Connects the PCRF to the SERVICE GATEWAY.
- SGi:** Connects the SERVICE GATEWAY to the Internet (globe icon).

Physical/Virtual Functions: The diagram indicates that the PCRF, SERVICE GATEWAY, and VAS are physical functions, while the S/PGW and BRAS are virtual functions.

POLICY CONTROL & CHARGING TURBO BOOST

Broadband subscribers typically sign up for the data plan that best suits their digital lifestyle. But there are always those moments when an extra boost of bandwidth is desired. For example, when snapping and sending photos from a sports venue with thousands of people doing the same, the data experience could be poor. Likewise, when streaming a full movie or downloading large files, real-time bandwidth-on-demand (BoD) comes in handy. The ability to obtain an on-demand speed upgrade for a limited duration is something many subscribers want and are willing to pay for.

DIFFERENTIATED OFFERINGS AND PERSONALIZED CUSTOMER EXPERIENCE



Key Benefits

- Increase bandwidth upsell opportunities
- Increase incremental ARPU through opt-in services
- Enhance your brand with services for the Digital Lifestyle

Turbo Boost in Action

- Operator detects QoE status and sends SMS offering turbo boost
- Subscriber selects BoD option via SMS or from operator portal
- BoD policy is applied for the specified time period
- Restore regular service plan when BoD time expires and send charge notification

Powered by Allot Service Gateway

- NetXplorer
- Subscriber Management Platform

Departments

Marketing/Operations

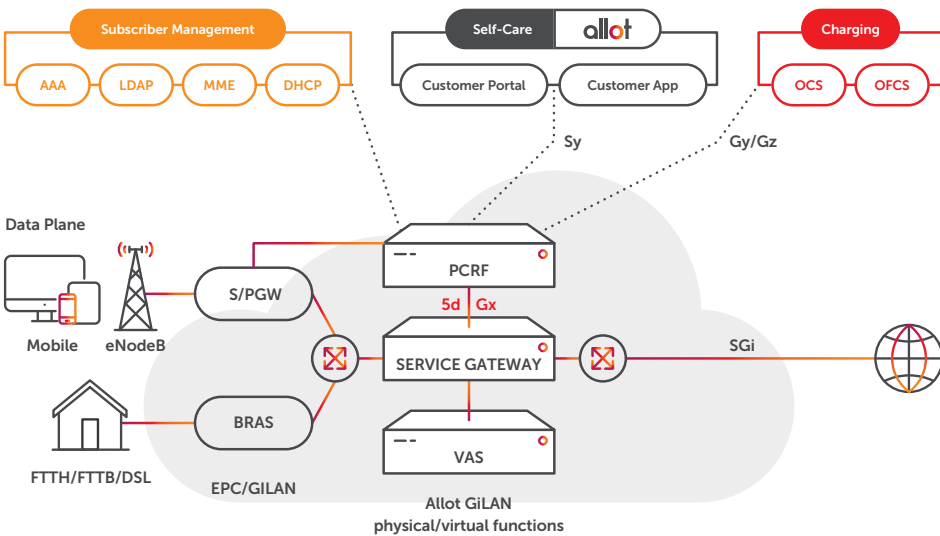
Technology

Mobile, Converged

POLICY CONTROL & CHARGING VOLUME-BASED CHARGING

Volume-based charging translates increased usage into proportional revenue growth for data service providers. It also helps them better regulate network utilization. For example, operators can offer a choice of data plans with megabyte or gigabyte caps priced according to the volume of data traffic allowed during a one-month period. Subscribers gain complete transparency regarding their actual data consumption plus the ability to control monthly costs. Further monetization opportunities open up when customers who are approaching their cap limit are notified and given the option to “top-up” their data cap for a fee, or to upgrade to higher usage plan. Volume-based charging also promotes fair use, as heavy users are no longer subsidized at the expense of others.

DIFFERENTIATED OFFERINGS AND PERSONALIZED CUSTOMER EXPERIENCE



Key Benefits

- Increase ARPU
- Close the gap between network usage and revenues
- Promote fair use and predictable utilization

Volume-based Charging in Action

- Meter subscriber usage in real-time
- Notify when usage approaches volume limit and redirect to top-up portal
- Customer may buy extra volume, upgrade service plan, or agree to overage fee
- Data cap automatically reset at end of billing period

Powered by Allot Service Gateway

- NetXplorer
- Subscriber Management Platform

Departments

Marketing/Operations

Technology

Mobile, Converged

TRAFFIC MANAGEMENT

Accurate traffic classification is a must to ensure Quality of Service in an era of encrypted traffic. Your brand is built on the QoS your customers experience every time they use the network. Allot's SmartTraffic QoE management enables intelligent and automated control of subscriber QoE at every point in your network. As a result, you save significantly on infrastructure costs, while delivering your network's best QoE – every time, every place.

Key Benefits

- Optimize utilization of existing infrastructure
- Improve customer experience
- Defer CAPEX expansion

QoE-based Congestion Management in Action

- Analyze network segment congestion
- Detect congested segments impacting QoE
- Implement prioritized congestion management policy
- Monitor and restore default policies when resolved

Powered by Allot Service Gateway

- NetXplorer

Departments

Engineering/Operations/
Marketing

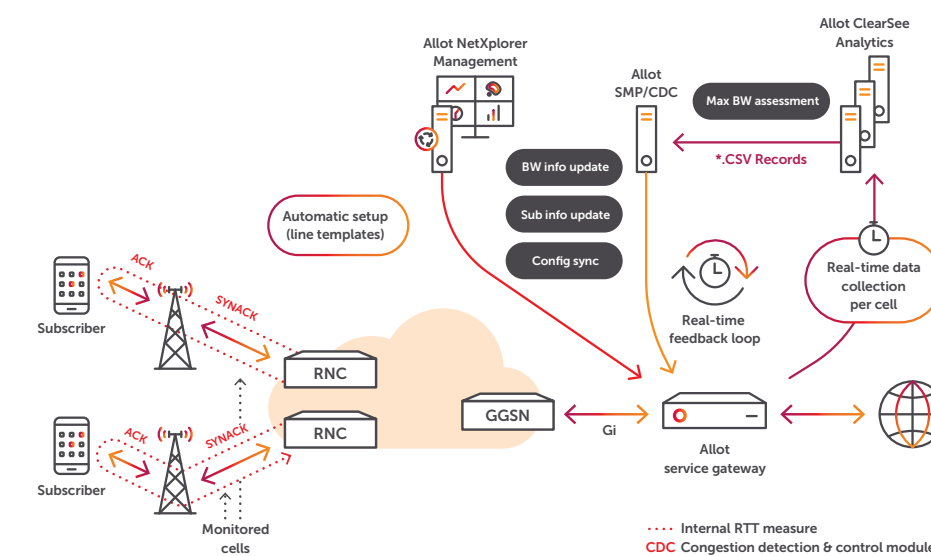
Technology

Fixed, Mobile, Converged

TRAFFIC MANAGEMENT QoE-BASED CONGESTION MANAGEMENT

Allot combines real-time monitoring of critical QoE indicators with policy-driven congestion control to maximize the quality of experience your deployed network can deliver at any given moment. When QoE indicators drop, our solution automatically shapes consumption while re-allocating available bandwidth according to your QoS or service plan policy. When the congestion is alleviated, the changes are rolled back to restore pre-configured settings

ENSURE QoS THROUGH TRAFFIC CLASSIFICATION AND OPTIMIZATION



Key Benefits

- Improve QoE for priority applications
- Improve resource utilization, save on CAPEX
- Save on OPEX by retiring other, more labor intensive, steering vendors
- Compliant with any VAS type; proxy, nonproxy, transparent, nontransparent

Layer 7 Steering for VAS Integration in Action

- Define Layer 7 steering policies
- Steer appropriate application traffic to or away from VAS delivery infrastructure
- Optimize network and application performance

Powered by Allot Service Gateway

- NetXplorer

Departments

Engineering/Operations/
Marketing

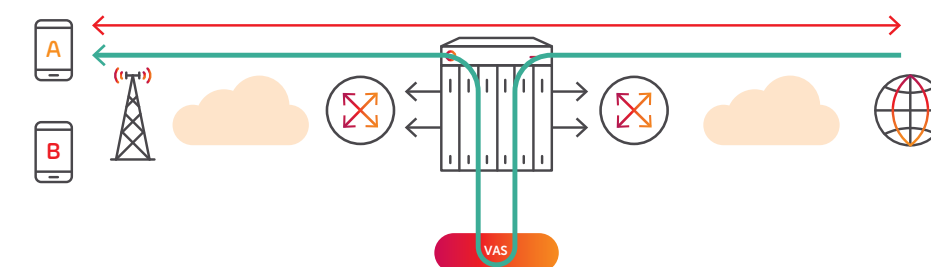
Technology

Fixed, Mobile, Converged

TRAFFIC MANAGEMENT LAYER 7 STEERING FOR VAS INTEGRATION

As service providers struggle to differentiate their services and improve their bottom line, optimizing resource utilization and improving customer QoE are increasingly important. The ability, for example, to automatically steer all incoming video traffic to a video optimization subsystem allows CSPs to deliver higher QoE at optimal network utilization and operational efficiency. Superior visibility and granular steering means only the traffic that needs to be steered will be steered, thereby minimizing the required VAS infrastructure and saving additional CAPEX.

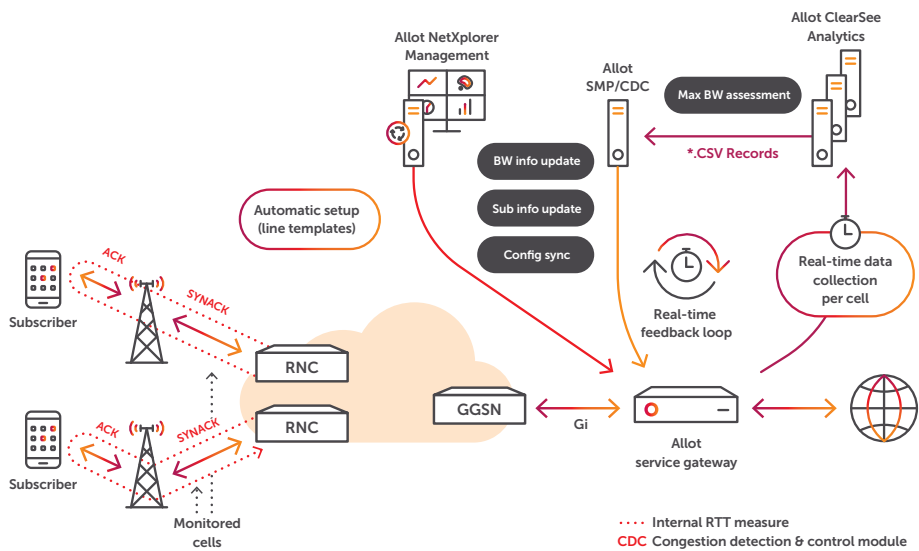
ENSURE QOS THROUGH TRAFFIC CLASSIFICATION AND OPTIMIZATION



TRAFFIC MANAGEMENT FAIR USE MANAGEMENT

Whether providing fixed or mobile connectivity, broadband service providers must constantly struggle to deliver fair and consistent QoE to all network subscribers, while refraining from making further investments in network resources. No single user is to be discriminated against, yet at the same time, none are to be allowed to abuse shared network resources at the expense of others. Fair use management ensures that no individual subscriber disrupts the service provided to others. It does so by managing throughput and subscriber QoE on the basis of congestion thresholds across the entire network.

ENSURE QoS THROUGH TRAFFIC CLASSIFICATION AND OPTIMIZATION



Key Benefits

- Reduce network congestion
- Ensure service availability/delivery even when network is congested
- Enhance customer satisfaction and reduce churn

Fair Use Management in Action

- Congestion threshold automatically triggers fair use policy enforcement
- Operator can rate-limit traffic of all subscribers in that part of network
- OR operator can rate-limit traffic per subscriber SLA
- Automatically restore regular policy when congestion subsides

Powered by Allot Service Gateway

- NetXplorer

Departments

Engineering/Operations/Marketing

Technology

Fixed, Mobile, Converged

Key Benefits

- Differentiate Enterprise offering
- Widen Enterprise customer base
- Increase Revenues

Multi-tenant Solution for Visibility & Control for Enterprise Customers in Action

- Monitor & report on network traffic and performance
- Implement prioritization policies
- Improve NW utilization, business critical application performance
- Secure enterprise connectivity

Powered by Allot Service Gateway

- NetXplorer

Departments

Engineering/Operations/Marketing

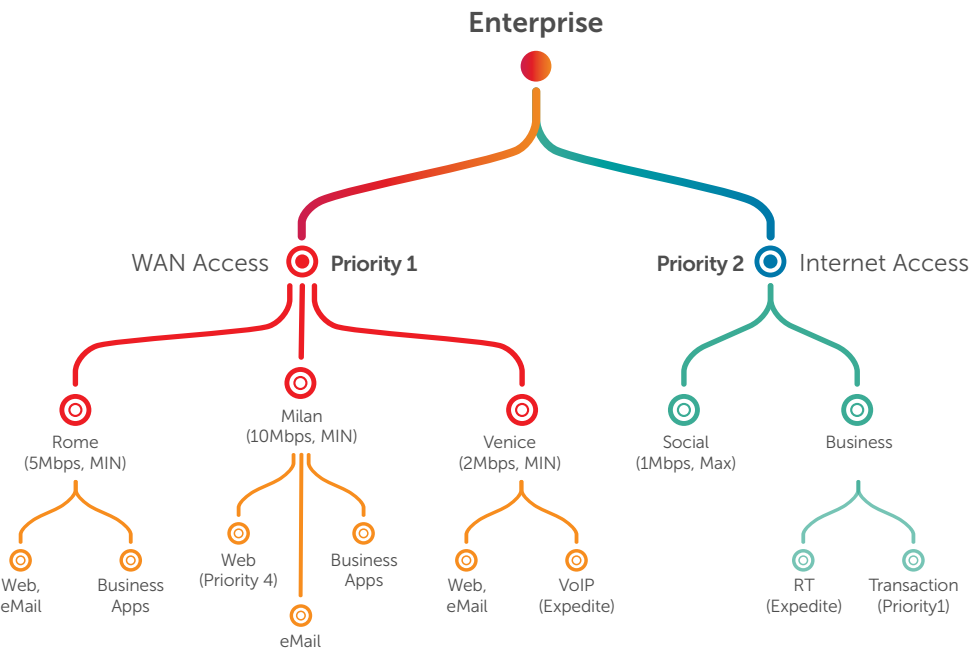
Technology

Fixed, Mobile, Converged

TRAFFIC MANAGEMENT MULTI-TENANT SOLUTION FOR VISIBILITY & CONTROL FOR ENTERPRISE CUSTOMERS

Enterprise customers are a potential source of significant revenue for CSPs. To better compete in this market, CSPs must offer greater value than just connectivity. By utilizing visibility, control and security through implementation of automated priority-based policies, congestion management and bidirectional security, CSPs can generate revenue by helping enterprises save money and increase worker efficiency.

TRAFFIC MANAGEMENT & ACCEPTABLE USE POLICY

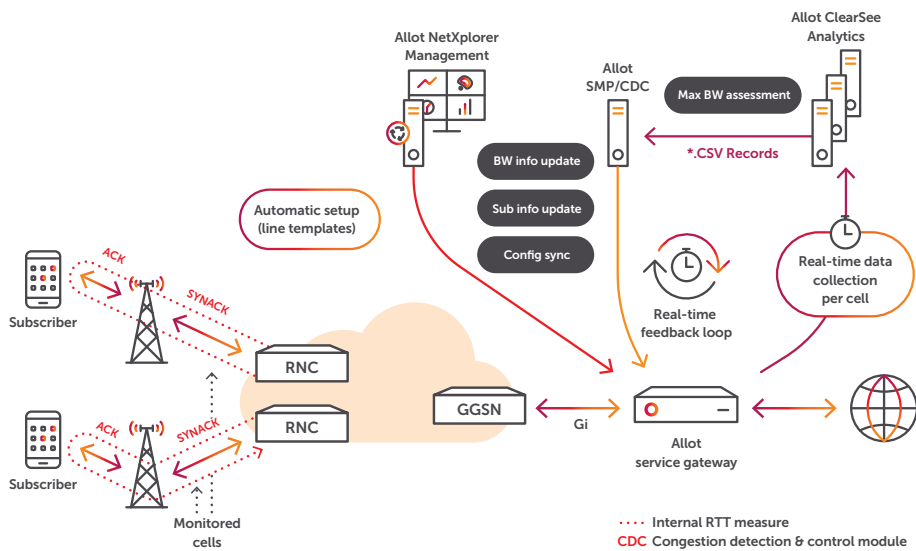


TRAFFIC MANAGEMENT

OTT VIDEO OPTIMIZATION

Video content providers always try to maximize resolution, even beyond the ability of many end-users to detect the difference in quality. This can put a serious strain on service providers' available bandwidth. At Allot we utilize policy-driven, Layer-7 aware bandwidth shaping to selectively reduce bandwidth availability which in turn triggers the video content providers' adaptive bit rate technology (ABR) to lower the video resolution. We achieve this via our lean, cost-effective, inline DPI solution that detects encrypted video and applies a corresponding bandwidth shaping policy. This powerful, small footprint solution enables SPs to deliver acceptable video quality, while optimizing the available bandwidth for all user and application needs.

ENSURE QoS THROUGH TRAFFIC CLASSIFICATION AND OPTIMIZATION



Key Benefits

- Save network bandwidth and contain costs
- Ensure consistently good video QoE
- Increase ARPU with value-added video services

OTT Video Optimization in Action

- Congestion threshold triggers optimization policy for streaming video content
- Enforce optimization policy for all video sessions, or only opt-in customers
- Shape bandwidth to trigger corresponding adaptive bit rate
- Deliver video stream optimized for receiving device and per SLA

Powered by Allot Service Gateway

- NetXplorer

Departments

Engineering/Operations/Marketing

Technology

Fixed, Mobile, Converged

Key Benefits

- Save CAPEX - optimize capacity utilization by shaping bandwidth based on AS destination
- Save CAPEX by automatically utilizing less costly links
- Save OPEX thru easier policy implementation

Autonomous Systems-BGP Awareness in Action

- Monitor AS utilization trends and costs
- Implement policies to shape bandwidth in real-time to match next hop capacity
- Implement policies to optimize routing via less costly links
- Expand capacity only when necessary

Powered by Allot Service Gateway

- NetXplorer

Departments

Engineering/Operations/Marketing

Technology

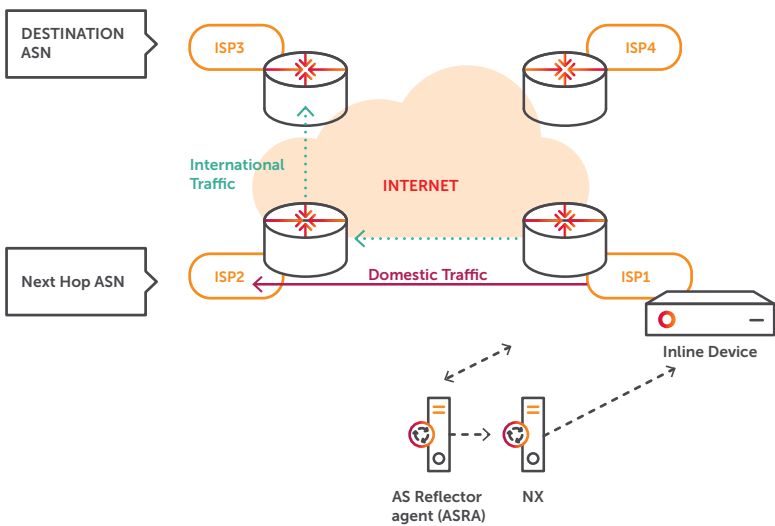
Fixed, Mobile, Converged

TRAFFIC MANAGEMENT

AUTONOMOUS SYSTEMS-BGP AWARENESS MANAGEMENT

Optimal utilization of existing capacity as well as preferential utilization of least cost routing can yield significant CAPEX savings. To achieve this without impacting QoE, CSPs must be able to see and classify traffic routing information in real-time and be able to implement optimal rerouting instantly. By optimizing the links used by bandwidth-hogging applications, we prevent them from overwhelming others. Using Allot's AS BGP Awareness enables CSPs to monitor and classify their outgoing traffic and reroute it and optimize its BW to automatically achieve the most cost-effective routing and capacity utilization.

ENSURE QoS THROUGH TRAFFIC CLASSIFICATION AND OPTIMIZATION



SECURITY VAS

Deliver a branded security service across multiple layers of security via a unified security service platform. The Allot Secure platform delivers unified client, gateway and network based security featuring a seamless customer experience for event handling, policy setting, and reporting as well as unified CSP management. Allot Secure^{NW} protects mobile, fixed, and converged customers at home, at work and on the go.

Key Benefits

- Frictionless onboarding and built-in customer engagement tools achieves ~50% uptake.
- Gain exceptionally high NPS
- Increase ARPU with incremental revenue from security services
- Strengthen customer loyalty with personalized services
- Protect your subscribers on-line

Security as a Service in Action

- Enables informed mass activation for opt-in and opt-out try and buy campaigns
- Delivers personalized customer engagement, reporting and notification tools
- Protects against adware, phishing, ransomware and other malicious payloads
- Deliver network-based security services

Powered by

- NetworkSecure
- HomeSecure
- EndpointSecure
- IoTSecure
- DDoS Secure

Departments

Security/Marketing

Technology

Fixed, Mobile, Converged

SECURITY VAS SECURITY AS A SERVICE

Consumer security awareness and concerns are growing with every headline describing a new type of malware or victim's story. Cybercrime has become big business, employing automation to increase the monetization of their nefarious activities. On the other hand, the unskilled consumer is left exposed with neither the time nor the inclination to deal with the complexities of security and point security products, they want someone else to do it for them and they are ready to pay. This is an opportunity for CSPs to step up and provide a valuable service that will be mutually beneficial by offering subscribers security as a service.

UNIFIED SECURITY FOR THE MASS MARKET



EndpointSecure



HomeSecure



NetworkSecure



IoTSecure



DDoSSecure

SECURITY VAS

SUBSCRIBER ENGAGEMENT FOR SECURITY VAS

In addition to providing effortless, network-based security for online mobile devices, Allot's NetworkSecure solution is also a platform for enhancing customer engagement – through personalized notifications and inserted info like icons or banners that attract users' attention and remind them that they are protected - and enable them to easily access self-service portals where they can configure their security settings and view reports on security events that were blocked. This engagement tool together with effective security and parental control has helped yield incredibly high NPS (Net Promoter Scores).

UNIFIED SECURITY FOR THE MASS MARKET



Key Benefits

- Increase VAS uptake/ revenue
- Increase Customer Satisfaction & loyalty
- Differentiate brand

OTT Video Optimization in Action

- Inject Icon
- Provide self-service portal
- Report on security events
- Deliver targeted marketing

Powered by

- NetworkSecure
- HomeSecure
- EndpointSecure

Departments

Security/Marketing

Technology

Fixed, Mobile, Converged

Key Benefits

- Extend network based security on and off net
- Increase Customer Satisfaction & loyalty
- Differentiate brand

Unified Security in Action

- Unified policy, event handling and reporting for client and network based security
- Seamlessly protect users when the switch to from cellular to wi-fi at home or on the go.
- Protects devices from on-line and off-line threats (e.g. syncing with an infected PC)

Powered by

- NetworkSecure
- HomeSecure
- EndpointSecure

Departments

Security/Marketing

Technology

Fixed, Mobile, Converged

SECURITY VAS

UNIFIED SECURITY

While network based security delivers effective security in addition to proven high adoption rates and significant service revenue it can only protect the traffic it inspects. To overcome this constraint, Allot has partnered with client security vendors to provide a unified solution that combines home gateway, client and network based security into a seamless security service. Allot Secure^{NW} is a security service delivery platform designed for CSPs that centrally manages and unifies multilayer, multivendor security. It unifies network-based security, home gateway security and security clients into your own branded security service. Allot Secure^{NW} delivers a seamless customer experience through a single interface for policy setting, reporting, and event handling.

UNIFIED SECURITY FOR THE MASS MARKET

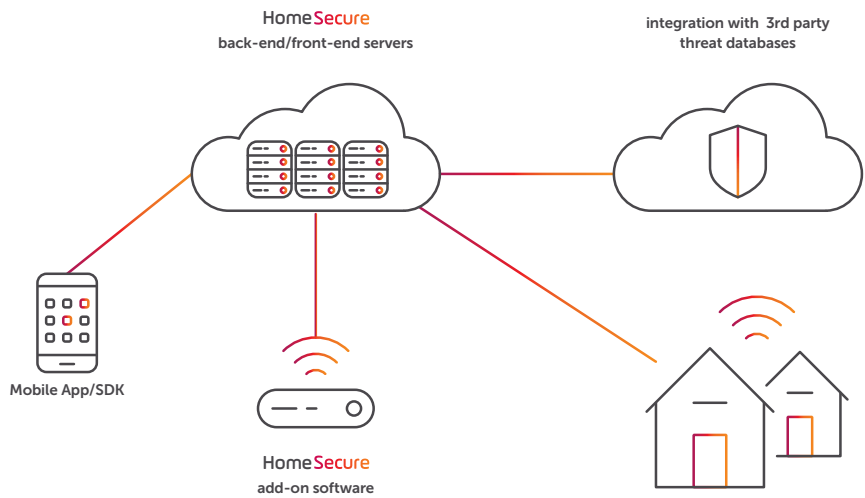


SECURITY VAS

SECURING THE SMART HOME

HomeSecure – a centrally managed thin agent that is remotely installed onto existing CPEs with less than 10% performance impact, protects networked devices in the home. Through machine learning techniques and visibility provided by the agent, all the devices within the home are identified, a default security policy is applied per device to protect against external threats and the home network is segregated to block lateral malware propagation.

THE SECURE SMART HOME



The agent also hardens the CPE against attack, protecting it from security vulnerabilities that can compromise the CPE itself, for example, password strength enforcement, open port analysis and protection and unauthorized access control. HomeSecure is the home gateway security layer of Allot Secure^{NW}

Key Benefits

- Deliver CSP branded security services that protects both IoT and end-user in the home
- Increase Customer Satisfaction & loyalty
- Increase ARPU with incremental revenue from security services

Securing the SmartHome in Action

- Protecting IoT and user devices from on-line external threats
- Segregating the home network to contain infected devices from lateral infection
- Hardening of CPE

Powered by

- HomeSecure

Departments

Security/Marketing

Technology

Fixed, Mobile, Converged

Key Benefits

- Increase ARPU with incremental revenue from premium, opt-in services
- Strengthen customer loyalty with personalized services
- Enhance brand image

Parental Control in Action

- Use self-care portal to set up safe-browsing profile for kids device(s)
- Monitor and filter Web traffic generated by opt-in devices in real time
- Analyze filtered traffic and enforce safe browsing rules in real time
- Send real-time notifications and monthly usage reports to parent

Powered by

- NetworkSecure
- HomeSecure
- EndpointSecure

Departments

Security/Marketing

Technology

Fixed, Mobile, Converged

SECURITY VAS

PARENTAL CONTROL

Parental Control service allows operators to provide peace of mind to parents who are concerned about the online activity of their children. Using a simple online setup screen, parents can control access to specific URLs and to a wide array of content categories such as gambling, pornography, dating sites, violence, racism and many others. They can also set time limits on browsing, set up different rules for each child's device, and adjust them at any time. Real-time notifications and monthly usage reports are all part of the service. Operators can deploy this opt-in service in multi tenancy mode that allows consumers to personalize their own security settings or in single tenancy mode that offers a standard set of security features for all subscribers

SECURING THE ONLINE EXPERIENCE



DDoS PROTECTION

Your network business and reputation depend on 100% service availability. That's why Allot helps you establish a completely automated, real-time defense against large scale inbound and outbound volumetric attacks. Allot accurately detects and mitigates zero-day DDoS attacks in seconds, without requiring supervision and before your infrastructure suffers costly service disruption or downtime.

Key Benefits

- Protect NW assets automatically, reducing OPEX
- Synergistic traffic management ensures consistent customer QoE even under attack
- Protect reputation by preventing SP from spreading IoT-based attacks
- Acquire comprehensive threat intelligence

Bidirectional DDoS Prevention in Action

- Detect known and unknown attacks in real-time; both incoming and outgoing
- Mitigate within seconds
- Preserve legitimate traffic

Powered by

- Service Gateway
- NetXplorer
- DDoS Secure
- Subscriber Management Platform

Departments

Security/Engineering/
Operations/Marketing

Technology

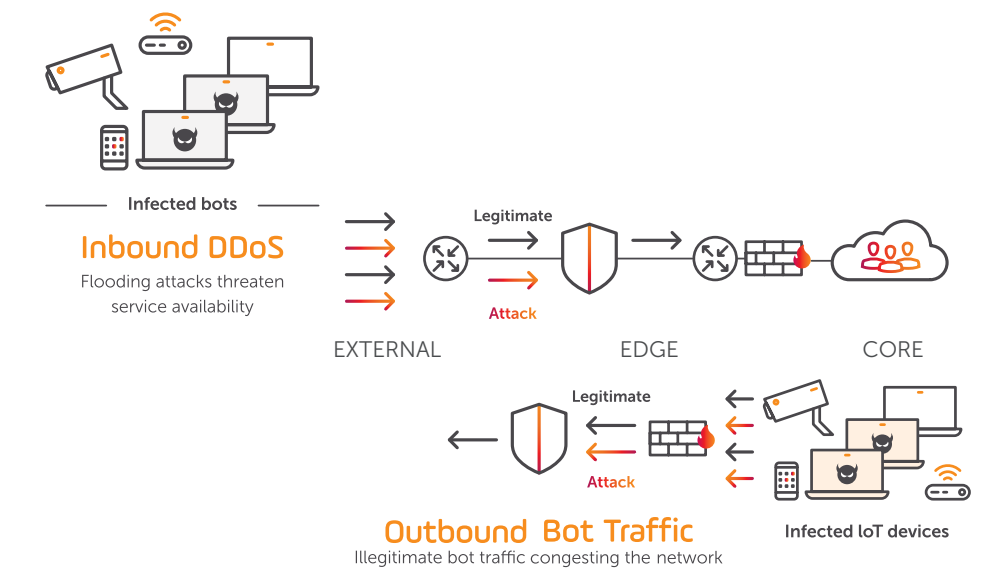
Fixed, Mobile, Converged

DDoS PROTECTION

BIDIRECTIONAL DDoS PREVENTION

DDoS attacks pose some of the most serious threats to your network, your services, your customers and your business. These complex, constantly mutating attacks continue to become larger and more menacing. With the growth of IoT, the threat has increased, and incidents now involve botnets created by hundreds of thousands of infected devices that disable services for millions of users. To address this, you need a robust solution you can rely on, that can guarantee detection and elimination of these attacks within seconds, before they are able to disrupt your network service

BIDIRECTIONAL DDOS PROTECTION



DDoS PROTECTION

DDoS SECURITY AS A SERVICE FOR ENTERPRISE

DDoS attacks pose some of the most serious threats to your enterprise customers’ networks, their services, their customers and their business. These complex, constantly mutating attacks continue to become larger and more menacing. With the growth of IoT, the threat has increased, and incidents now involve botnets created by hundreds of thousands of infected devices that disable services for millions of users. To address this, you need a robust solution you can rely on, that can guarantee detection and elimination of these attacks within seconds, before they are able to disrupt your network service.

Key Benefits

- Differentiate connectivity services
- Protect Enterprise customers
- Protect customers’ reputation

Bidirectional DDoS Prevention in Action

- Detect known and unknown attacks in real-time; both incoming and outgoing
- Mitigate within seconds
- Preserve legitimate traffic

Powered by

- Service Gateway
- NetXplorer
- DDoS Secure
- Subscriber Management Platform

Departments

Security/Engineering/
Operations/Marketing

Technology

Fixed, Mobile, Converged

Key Benefits

- Differentiate wholesale connectivity services
- Protect customers’ NW assets
- Protect customers’ reputation

Bidirectional DDoS Prevention in Action

- Detect known and unknown attacks in real-time; both incoming and outgoing
- Mitigate within seconds
- Preserve legitimate traffic

Powered by

- Service Gateway
- NetXplorer
- DDoS Secure
- Subscriber Management Platform

Departments

Security/Engineering/
Operations/Marketing

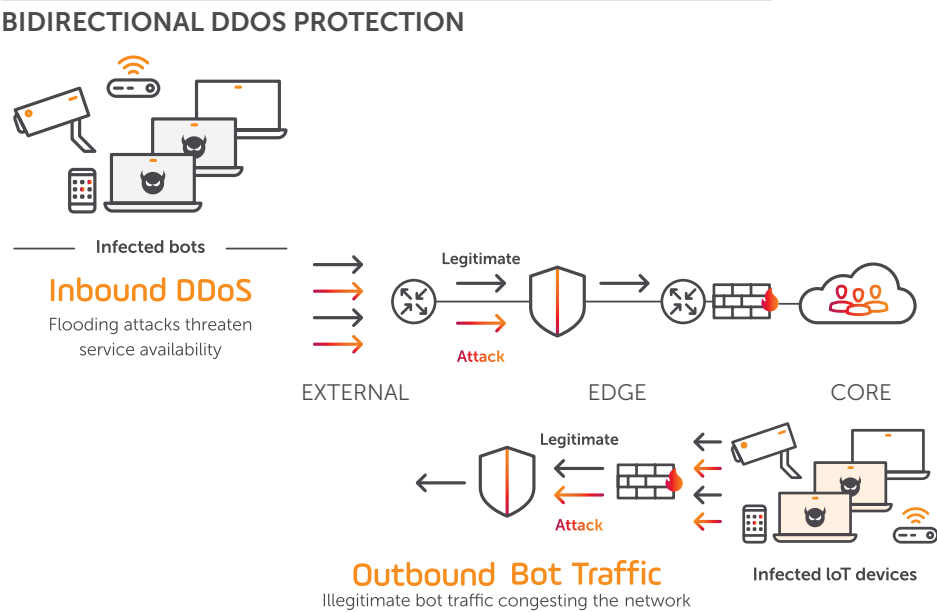
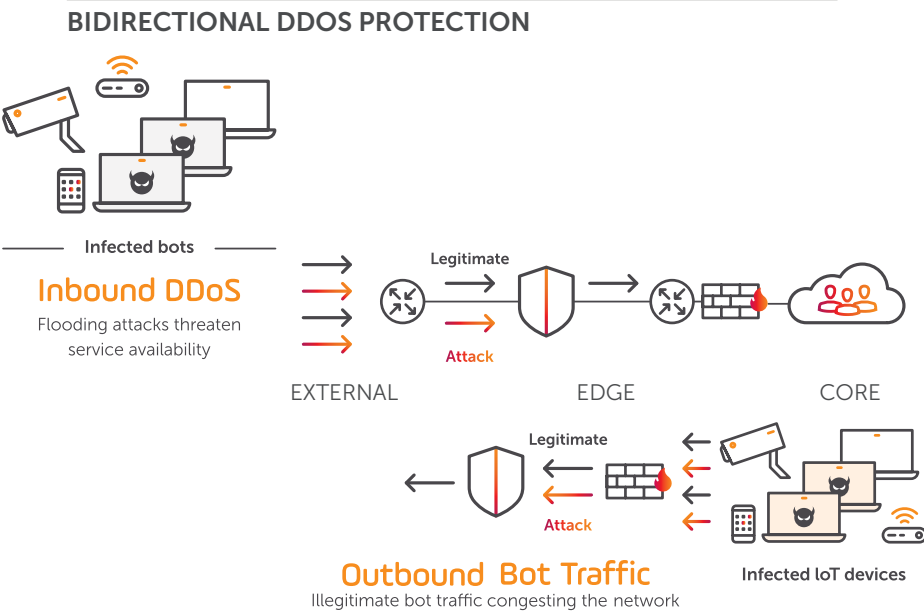
Technology

Fixed, Mobile, Converged

DDoS PROTECTION

DDoS SECURITY AS A SERVICE FOR INTERCONNECT CARRIERS

DDoS attacks pose some of the most serious threats to your customers’ networks and their business. These complex, constantly mutating attacks continue to become larger and more menacing. With the growth of IoT, the threat has increased, and incidents now involve botnets created by hundreds of thousands of infected devices that disable services for millions of users. To address this, you need a robust solution you can rely on, that can guarantee detection and elimination of these attacks within seconds, before they are able to disrupt your network service.



IoT SECURITY

Capitalize on new opportunities created by the Internet of Things by meeting IoT control and security challenges head on. Allot helps you protect your IoT service network and increase operational efficiency, while enabling value added services, such as IoT security tiers and IoT analytics that give your offering a competitive edge and generate new revenue.

Key Benefits

- Increase ARPU through value added services
- Differentiate your IoT offering
- Meet growing demand for IoT security services

IoT Security as a Service in Action

- Policy definition for behavior assurance
- Behavioral analysis and anomaly detection
- Bot and DDoS protections
- Data-driven decisions for informed troubleshooting

Powered by

- Service Gateway
- NetXplorer
- IoTSecure
- DDoS Secure
- ClearSee
- Subscriber Management Platform

Departments

Security/Operations/Marketing

Technology

Fixed, Mobile, Converged

IoT SECURITY

IoT SECURITY AS A SERVICE

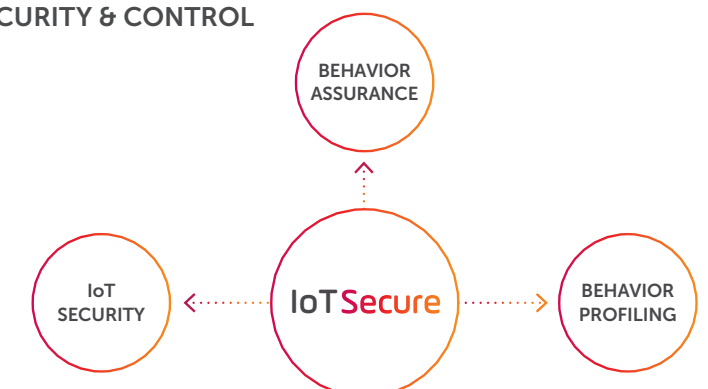
Security is the number one concern for Enterprises that want to deploy or extend their IoT networks. CSPs are ideally positioned to deliver network-based security services as additional assets to their connectivity services to increase IoT monetization and differentiate their offering for an additional competitive advantage. IoT network-based Value Added Services are fully aligned with the operator's expertise and core business. Allot's IoTSecure delivers carrier-class security, behavior analysis, and traffic intelligence and control. It enables your customers to configure the following services and features through a customer self-care portal.

IoT Security: A network-based security solution that protects against malware and botnets and enables remote remediation of suspect devices through smart quarantine that limits connectivity only to remote diagnostic and remediation systems.

Behavior Assurance: The ability for an enterprise to define policies that manage IoT deployments. This includes whitelisting of communications, protocols, and traffic patterns of IoT devices with their legitimate servers.

Behavior Profiling and Anomaly detection: An artificial intelligence approach to IoT analytics for detecting SIM misuse and data plan protection and identifying compromised or malfunctioning IoT devices.

IoT VISIBILITY, SECURITY & CONTROL



IoT SECURITY

IMPROVE IoT OPERATIONAL EFFICIENCY

Operational efficiency is key to scaling and protecting the communications infrastructure efficiently and supporting the rapid growth of IoT and related infrastructure investments. IoTSecure provides IoT aware network analytics to support informed investment decisions, expedite troubleshooting, and verify that customers meet the terms and conditions of an IoT Data Plan. In addition, QoE based congestion control provides adaptive traffic management to ensure user QoE in the face of growing IoT deployments on a shared infrastructure.

Key Benefits

- Improve operational efficiency through visibility and control of connected IoT deployments
- Data driven traffic management, capacity planning and troubleshooting
- Prevent revenue leakage

IoT Operational Efficiency in Action

- Gain visibility on IoT behavior to manage and promote data plan
- Monitor SIM behavior
- Alert and block upon anomalous data traffic
- QoE-based congestion control

Powered by

- Service Gateway
- NetXplorer
- IoTSecure
- DDoS Secure
- ClearSee
- Subscriber Management Platform

Departments

Security/Operations/Marketing

Technology

Fixed, Mobile, Converged

Key Benefits

- Protect the mobile infrastructure from IoT borne attacks
- Protect IoT deployments from attacks
- Prevent damage to reputation

Protect Infrastructure from IoT Borne Attacks in Action

- Profile and monitor behavior of IoT traffic
- Apply behavioral analysis and anomaly detection
- Identify and quarantine anomalous device traffic
- Bidirectional DDoS protection
- IoT Bot protection

Powered by

- Service Gateway
- NetXplorer
- IoTSecure
- DDoS Secure
- ClearSee
- Subscriber Management Platform

Departments

Security/Operations/Marketing

Technology

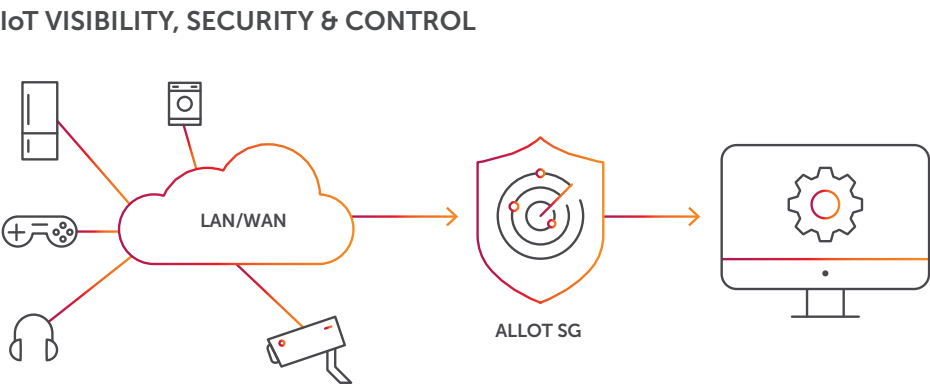
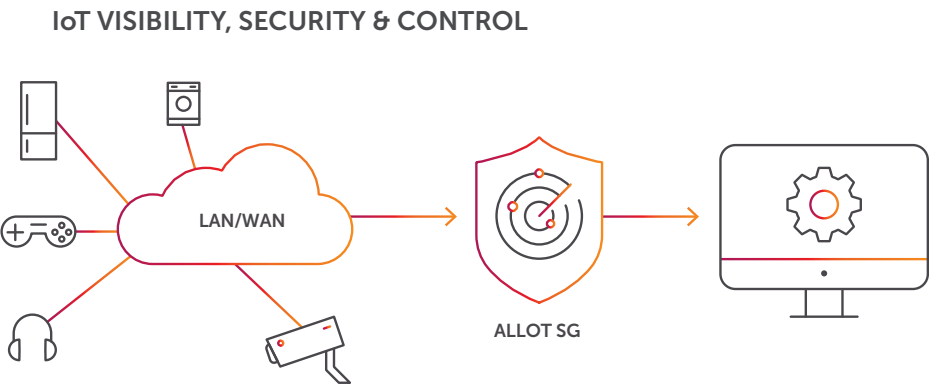
Fixed, Mobile, Converged

IoT SECURITY

PROTECT INFRASTRUCTURE FROM IoT BORNE ATTACKS

IoTSecure ensures resilience of the CSP infrastructure and maintains QoE for customers who rely on a carrier's network. The volume of IoT-borne DDoS traffic can have a devastating impact on the communications infrastructure it traverses and the QoE of customers who share the same telecommunications infrastructure. Allot IoTSecure DDoS protection is unique as it provides advanced, behavior-based bidirectional detection and mitigation in less than 60 seconds

This protects the infrastructure against DDoS attacks initiated from internal and external sources and maintain the QoE of bystanders sharing the same network.



Regulatory Compliance

Your communications network is subject to a wide range of regulations that require timely and firm compliance. With the power to inspect all traffic on your network, and to forward and filter, Allot's SmartRegulator helps you successfully navigate the changing regulatory landscape.

Key Benefits

- Get off and stay off spammer blacklists
- Reduce complaints from other operators
- Avoid unnecessary investment in content-based spam filtering solutions

Anti-spam in Action

- Detect anomalous behavior consistent with spamming
- Quarantine spammer into service plan that blocks, rate-limits, or redirects the spam traffic
- Notify subscriber via SMS and/or email
- Redirect spammer to clean-up portal to remove spambot infection

Powered by

- Service Gateway
- NetXplorer
- ClearSee

Departments

Security/Operations

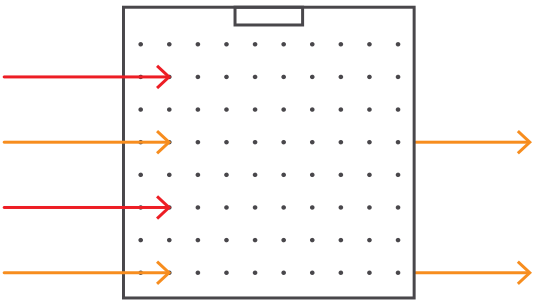
Technology

Fixed, Mobile, Converged

REGULATORY COMPLIANCE ANTI-SPAM (BLACKLIST PREVENTION)

Outbound spam is the primary cause of service provider blacklisting. While DNS blacklists (DNSBL) are widely used as a first line of defense, they are mostly ineffective as they rely solely on the spamming IP address. Consequently, when spam originates from the service provider network the spamming IP is blacklisted, and many innocent subscribers are also impacted, either by having inherited a blacklisted IP (via DHCP) or by sharing the same "public" IP (behind the same NAT IP) as the spammer. Blacklist prevention obviates this problem by detecting the spamming subscriber and automating the process of notification and remediation of infected devices

IOT VISIBILITY, SECURITY & CONTROL



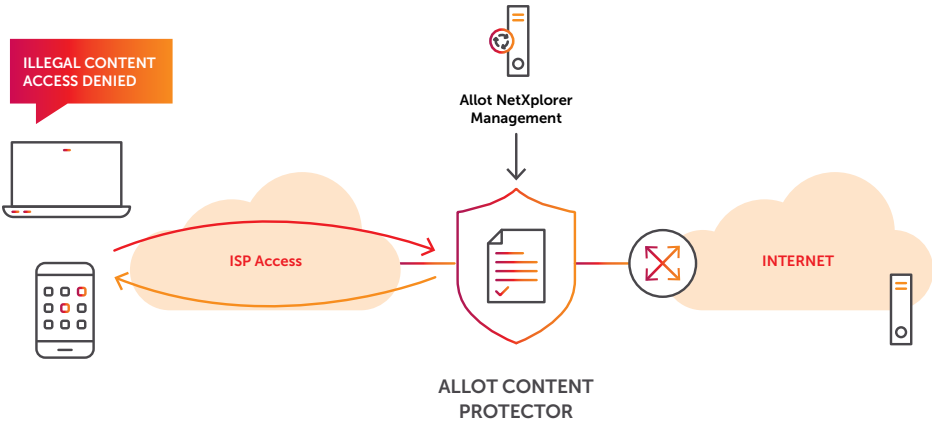
ALLOT SPAM FILTERING

REGULATORY COMPLIANCE

BLACKLIST URL FILTERING

When government regulations forbid your network from providing access to illegal or harmful content, Allot's carrier-class URL filtering service gives you the flexibility to comply with regulatory requirements and to proactively provide a safer and more protected Internet environment for your customers. With the power to inspect all traffic on your network, Allot's URL filtering capabilities ensure that blacklisted and illegal Internet sites are blocked in real time.

BLOCK UNDESIRABLE SITES



Key Benefits

- Comply with Regulations
- Enhance reputation by protecting users from malicious content
- Support millions of users without impacting performance

Blacklist URL Filtering in Action

- Integrate with authorized blacklists such as Internet Watch Foundation (IWF)
- Automate blacklist updates ensure constant compliance
- Easily integrate additional blacklists

Powered by

- Service Gateway
- NetXplorer
- ClearSee

Departments

Security/Operations

Technology

Fixed, Mobile, Converged

Key Benefits

- Comply with Regulations
- Enhance reputation by protecting users from malicious content
- Support millions of users without impacting performance

Unified Regulatory Compliance in Action

- Obtain granular, big data visibility into network, user and application behavior
- Block illegal content and applications
- Retain unlimited amount of detailed usage records
- Protect Network infrastructure against both inbound and outbound DDoS attacks

Powered by

- Service Gateway
- NetXplorer
- ClearSee

Departments

Security/Operations

Technology

Fixed, Mobile, Converged

REGULATORY COMPLIANCE

UNIFIED REGULATORY COMPLIANCE

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.

UNIFIED REGULATORY COMPLIANCE



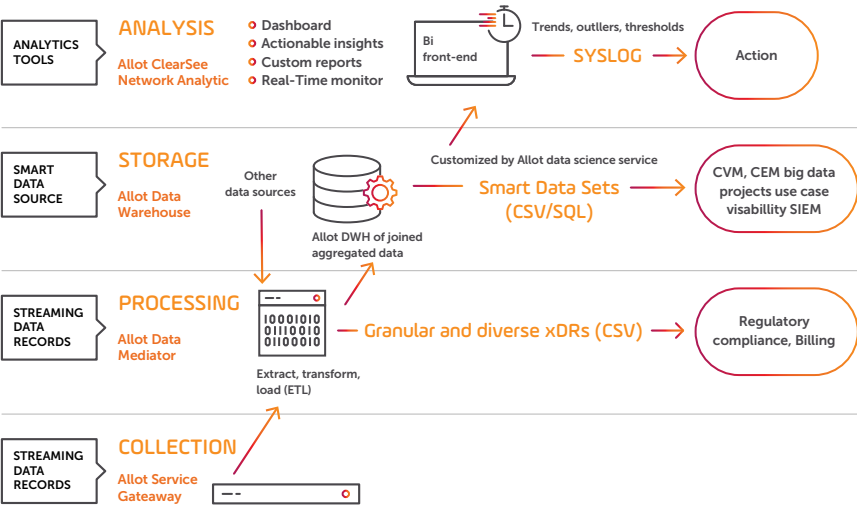
REGULATORY COMPLIANCE

USAGE RECORDS STORE & RETRIEVE

Regulatory compliance has become mission critical for national authorities and service providers 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.

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.

GRANULAR VISIBILITY INTO ALL APPLICATION AND USER TRAFFIC



Key Benefits

- Comply with Regulations

Usage Records Store & Retrieve Action

- Lawfully intercept and block dangerous traffic
- Filter out illegal and harmful URLs
- Record and store per-user online activity records in Big Data database
- Provide interface for information lookup

Powered by

- Service Gateway
- NetXplorer
- ClearSee

Departments

Security/Operations

Technology

Fixed, Mobile, Converged

Key Benefits

- Comply with regulations
- Increase customer satisfaction and loyalty
- Generate additional revenue via new upsell opportunities

Bill Shock in Action

- Detect roaming when data session is initiated and redirect to operator portal
- Option 1:** Purchase a package that blocks certain content when roaming
- Option 2:** Acknowledge additional charges and continue under current service plan
- Option 3:** Purchase a discounted data roaming package for a limited time

Powered by

- Service Gateway
- NetXplorer
- ClearSee
- Subscriber Management Platform

Departments

Security/Operations

Technology

Mobile, Converged

REGULATORY COMPLIANCE

BILL SHOCK PREVENTION

When faced with an unexpected high charge for data roaming services, customers are likely to be in for a shock. Valid or not, they often contest the charges claiming they were not informed by the operator. Hoping to keep customer satisfaction and retention high, operators may end up waiving the extra charges and pick up the tab themselves, resulting in significant revenue loss. This phenomenon has resulted in legislation and regulations to prevent bill shock. Bill shock prevention service enables operators to notify roaming subscribers of data session costs in real time, and require that they acknowledge these charges before establishing a connection. Customers feel more in control when charging schemes are transparent and known up front.

FINAL WORD

With over 20 years' experience empowering service providers to get more out of their networks and to manage them more efficiently, we enable network operators to clearly see and understand their networks from within. Allot provides its customers with the tools to optimize, innovate, and capitalize on every opportunity; to learn about users and network behaviors; to improve quality of service and reduce costs; and to detect security breaches to protect their own networks and their users from attacks. All of this is achieved while increasing value to customers and deploying new services more quickly than ever before.

When visibility is clear and network intelligence is accurate, you can make smart decisions in real time to truly manage your network, engage your customers and innovate with new services.

Allot's multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises globally in the most demanding environments. We support our customers' requirements to scale efficiently and keep pace with evolving network architectures by offering the most scalable platforms in the market including tested NFV compliant solutions.

For more information, visit: <https://www.allot.com/service-providers/>

