allot Secure ^{NW}
CSP Use Cases

CONTENTS

Security is the next big opportunity for operators to enhance the digital experience of their customers. Our cybersecurity solution provides 'peace of mind' for consumers.

Francisco Cayuela,
Vice President Sales,
Spain and LATAM at Allot.

INTRODUCTION

Allot is a leading global provider of innovative network intelligence and security solutions for service providers, helping you to provide enhanced value to your customers. Our solutions, deployed globally, deliver network and application analytics, traffic control and shaping, and network-based security services.
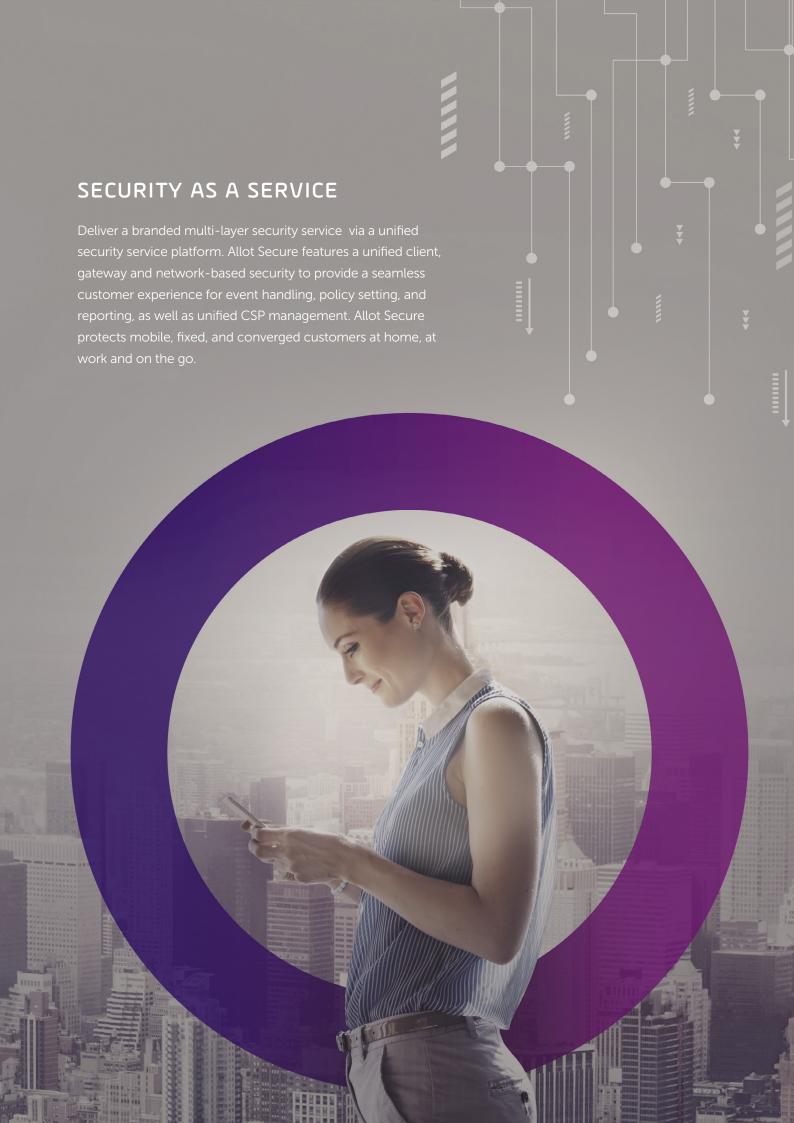
The use cases in this booklet focus on Allot Secure, our network-based security platform, which disrupts the security industry by positioning CSPs as leading Security-as-a-Service providers with market penetration exceeding 50% and protecting over 20 million subscribers worldwide. Recently introduced modules, IoTSecure and HomeSecure, enable service providers to secure enterprise and consumer IoT deployments at the network layer, in both fixed and mobile networks. Allot Secure delivers anywhere, any device, any threat protection and generates value-added-service revenue of 10-15% on top of pure connectivity.

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

Allot is your partner for delivering high quality network intelligence and security solutions.services.

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

o   Mobile Security Service

o   Home Security Service

o   IoT Security

o   DDoS Protection

SECURITY AS A SERVICE

Deliver a branded multi-layer security service via a unified security service platform. Allot Secure features a unified client, gateway and network-based security to provide a seamless customer experience for event handling, policy setting, and reporting, as well as unified CSP management. Allot Secure 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 AS A SERVICE
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

Endpoint Secure   Home Secure   Network Secure   IoT Secure   DDoS Secure

SECURITY AS A SERVICE
SUBSCRIBER ENGAGEMENT FOR SECURITY AS A SERVICE

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).

Key Benefits

- o Increase security services uptake/revenue
- o Increase Customer Satisfaction & loyalty
- o Differentiate brand

Subscriber Engagement in Action

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

Powered by

- o NetworkSecure
- o HomeSecure
- o EndpointSecure

Departments

Security/Marketing

Technology

Fixed, Mobile, Converged

UNIFIED SECURITY FOR THE MASS MARKET

EndpointSecure   HomeSecure   NetworkSecure

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 AS A SERVICE
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 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 delivers a seamless customer experience through a single interface for policy setting, reporting, and event handling.

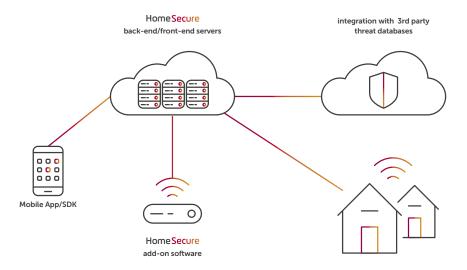### UNIFIED SECURITY FOR THE MASS MARKET

EndpointSecure   HomeSecure   NetworkSecure

SECURITY AS A SERVICE
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

HomeSecure
back-end/front-end servers

integration with 3rd party
threat databases

Mobile App/SDK

HomeSecure
add-on software

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.

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

- Deliver CSP branded cybersecurity services that protects IoT devices, end-user devices and hardens the CPE

- Zero-touch, clientless onboarding

- Very high adoption rates

- Increase customer satisfaction & brand loyalty, reduce churn and differentiate

- Increase ARPU with incremental revenues

Provision of Cybersecurity and Parental controls

- Protect users from malware-based internet threats including ransomware, botnets, anti-virus, anti-phishing

- Protecting children from accessing inappropriate or unwanted internet content, per device, website filtering by category

- Defining internet-access times, device blocking

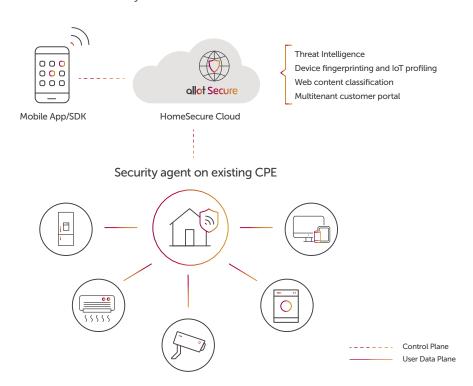## Powered by

HomeSecure

Departments

Marketing/Network/CPE

Technology

Fixed

SECURITY AS A SERVICE
FIXED BROADBAND CYBERSECURITY AND PARENTAL CONTROLS

HomeSecure - A large Asian Tier 1 provider sought a cybersecurity and parental controls solution for its fixed broadband customers. The provider had received feedback from its customers that one of their most critical needs was cybersecurity. Furthermore, with children being such predominant internet users, protecting their access was viewed as being important and in line with the social values of the country.

Mobile App/SDK   HomeSecure Cloud

Threat Intelligence
Device fingerprinting and IoT profiling
Web content classification
Multitenant customer portal

Security agent on existing CPE

Control Plane
User Data Plane

HomeSecure has a centrally managed thin agent that is remotely installed onto the router, protecting the networked devices from cyberattacks in consumer homes. The agent hardens the CPE against attack, protecting it from security vulnerabilities that can compromise the CPE itself. HomeSecure also provides parental controls that can be configured by the user to block more than 120 categories as well as defining internet access times or block the device altogether.

SECURITY AS A SERVICE
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

Key Benefits

o   Increase ARPU with incremental revenue from premium, opt-in services

o   Strengthen customer loyalty with personalized services

o   Enhance brand image

Parental Control in Action

o   Use self-care portal to set up safe-browsing profile for kids device(s)

o   Monitor and filter Web traffic generated by opt-in devices in real time

o   Analyze filtered traffic and enforce safe browsing rules in real time

o   Send real-time notifications and monthly usage reports to parent

Powered by

o   NetworkSecure

o   HomeSecure
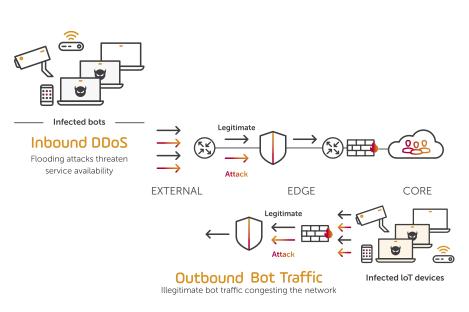
o   EndpointSecure

Departments

Security/Marketing

Technology

Fixed, Mobile, Converged

DDoS PROTECTION

Your network, business and reputation depend on 100% service availability. Allot's DDoS Secure helps you establish a completely automated, real-time defense against large scale inbound and outbound volumetric attacks of any size, from any direction. It accurately detects and mitigates zero-day DDoS attacks in seconds, without requiring supervision and before infrastructure suffers costly service disruption or downtime. With the explosive growth in potentially weaponized IoT devices and increased access speeds associated with 5G, you will need DDoS Secure's combined network behavior anomaly detection with host behavior anomaly detection.

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

Infected bots

Inbound DDoS
Flooding attacks threaten service availability

Legitimate

Attack

EXTERNAL   EDGE   CORE

Legitimate

Attack

Outbound Bot Traffic
Illegitimate bot traffic congesting the network

Infected IoT devices

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

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

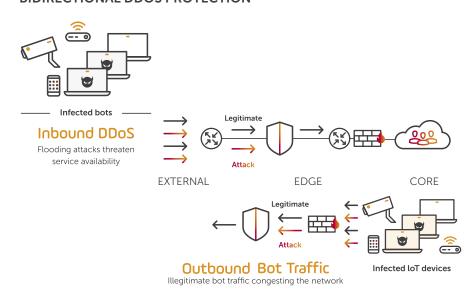## Departments

Security/Engineering/
Operations/Marketing

Technology

Fixed, Mobile, Converged

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.

BIDIRECTIONAL DDOS PROTECTION

Infected bots

Inbound DDoS
Flooding attacks threaten service availability

Legitimate

Attack

EXTERNAL   EDGE   CORE

Legitimate

Attack

Infected IoT devices

Outbound Bot Traffic
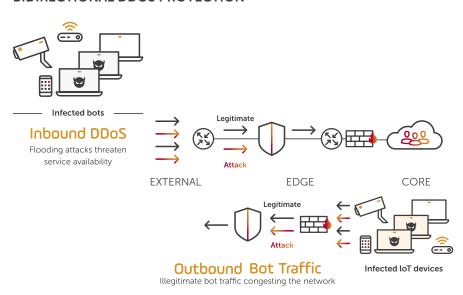Illegitimate bot traffic congesting the network

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.

BIDIRECTIONAL DDOS PROTECTION

Infected bots

Inbound DDoS
Flooding attacks threaten service availability

Legitimate

Attack

EXTERNAL   EDGE   CORE

Legitimate

Attack

Outbound Bot Traffic
Illegitimate bot traffic congesting the network

Infected IoT devices

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

IoT SECURITY

Capitalize on new opportunities created by the emerging needs of IoT. Meet the challenges of managing and securing IoT devices on a mass scale with IoTSecure. IoTSecure protects your IoT service network and increases 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.

IoT SECURITY
IoT SECURITY AS A SERVICE
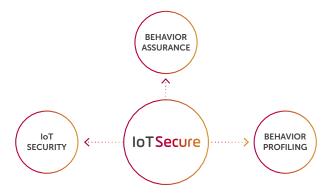
Security is the number one concern for Enterprises that want to deploy or extend their IoT networks. CSPs are ideally positioned to deliver network-based security services as additional assets to their connectivity services to increase IoT monetization and differentiate their offering for an additional 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

Key Benefits

o Increase ARPU through value added services

o Differentiate your IoT offering

o Meet growing demand for IoT security services

IoT Security as a Service in Action

o Policy definition for behavior assurance

o Behavioral analysis and anomaly detection

o Bot and DDoS protections

o Data-driven decisions for informed troubleshooting

Powered by

o Service Gateway

o NetXplorer

o IoTSecure

o DDoS Secure

o ClearSee

o Subscriber Management Platform

Departments

Security/Operations/Marketing

Technology

Fixed, Mobile, Converged

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

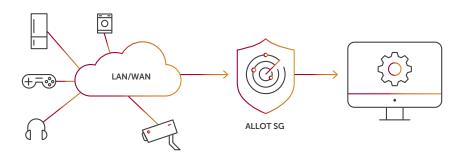## Departments

Security/Operations/Marketing

Technology

Fixed, Mobile, Converged

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.

IoT VISIBILITY, SECURITY & CONTROL

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.

IoT VISIBILITY, SECURITY & CONTROL

LAN/WAN

ALLOT SG

Key Benefits

o Protect the mobile infrastructure from IoT borne attacks

o Protect IoT deployments from attacks

o Prevent damage to reputation

Protect Infrastructure from IoT Borne Attacks in Action

o Profile and monitor behavior of IoT traffic

o Apply behavioral analysis and anomaly detection

o Identify and quarantine anomalous device traffic

o Bidirectional DDoS protection

o IoT Bot protection

Powered by

o Service Gateway

o NetXplorer

o IoTSecure

o DDoS Secure

o ClearSee

o Subscriber Management Platform

Departments

Security/Operations/Marketing

Technology

Fixed, Mobile, Converged

ABOUT ALLOT

Allot is a leading provider of innovative network intelligence and security solutions that empower communications service providers (CSPs) and enterprises worldwide to enhance the value they bring to their customers. With over 20 years of proven success, our solutions turn network, application, usage and security data into actionable intelligence that make our customers' networks **smarter** and their users more **secure**.

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. Recently introduced modules, IoTSecure and HomeSecure, enable service providers to secure enterprise and consumer IoT deployments at the network layer, in both fixed and mobile networks. Allot Secure delivers anywhere, any device, any threat protection and generates value-added-service revenue of 10-15% on top of pure connectivity.

Our **Allot Smart** solution suite, powered by inline DPI technology, generates insightful intelligence that empowers our customers 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 our customers' end-users. Using Allot Smart, our customers have lowered access bandwidth costs by 10%, deferred capacity expansions by 1-2 years and reduced revenue leakage by 15%.

Allot's multi-service platforms are deployed globally, in the most demanding environments, by over 500 mobile, fixed and cloud service providers and over a thousand enterprises. We support evolving network architectures by offering the most flexible platforms in the market, including COTS hardware, software only and field-proven, fully NFV compliant solutions.

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

Sep 2021