allot Smart

SmartSentinel: Digital Enforcement for Governments

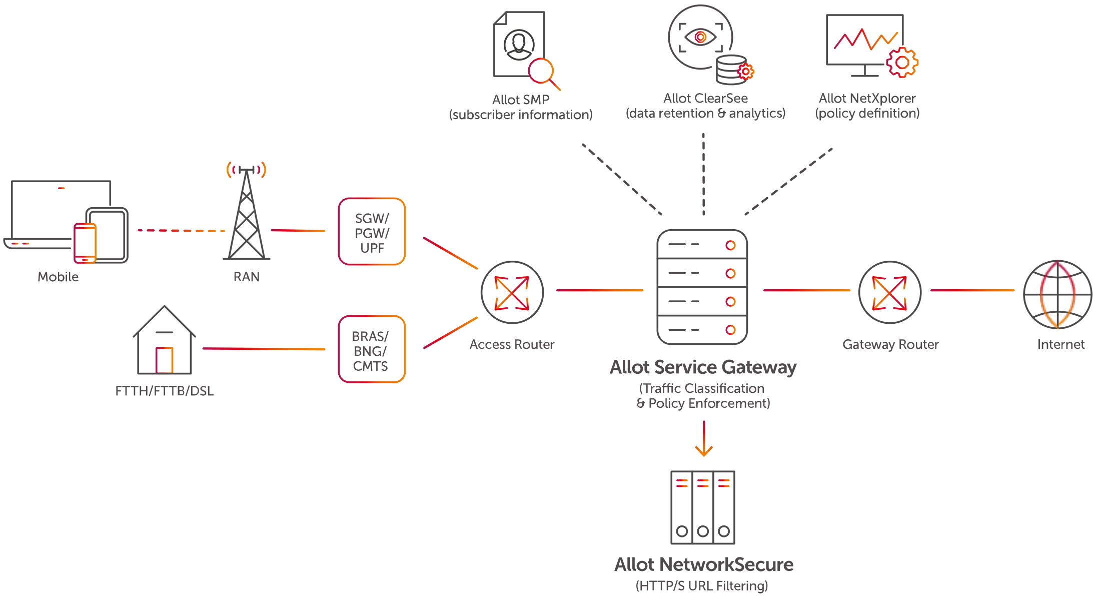
Use Cases

CONTENTS

INTRODUCTION

The cyber age presents nations with the challenge of extending their laws to the internet and exercising their digital sovereignty. Governments struggle to maintain a balance between the free flow of information and lawful restrictions that aim to prevent criminal abuse of the internet. Access to offensive content, such as child pornography, must be denied; criminals using the internet for their illegal needs must be detected; and national infrastructure, such as telecom networks, must be protected.

UNIFIED MANAGEMENT ARCHITECTURE



VPN AND ANONYMIZER CONTROL

Usage of VPNs and anonymizers has become standard operating procedure for criminal elements that wish to access illegal content. Whether trying to access offensive child pornography or simply watch live sports events while violating usage rights, they use these tools to thwart detection, remain anonymous, and avoid prosecution. The best solution in the market addressing this challenge is Allot SmartSentinel. Powered by world-leading DPI engine that incorporates two and a half decades of DPI knowledge, machine learning and big data technologies, Allot SmartSentinel identifies VPNs and anonymizer sessions with high precision and successfully blocks their access to illegal content.

Key Benefits

- High precision VPNs and anonymizers detection
- ophisticated blocking mechanisms that overcome the most advanced evasive techniques
- Inherent reporting and analytics used as lead information for follow up investigations or evidence in courts

In Action

- Gain detailed visibility into usage of VPNs and anonymizers throughout all monitored networks
- Apply policies from a central control center to overcome VPNs blocking circumvention tactics through Machine Learning powered DPI
- Prevent access to illegal content and usage of illegal applications encapsulated within VPNs
- Uncover the identities of criminals using VPNs and anonymizers

Powered by

- Service Gateway
- NetXplorer
- SMP
- ClearSee

Departments

Telecom Regulators/
Law Enforcement

Technology

Fixed, Mobile, Converged

VOIP MANAGEMENT AND CONTROL

Criminals often use VoIP communications to hide illegal activities from law enforcement agencies. Regulators and governments need ways to steer criminal and terrorist VoIP traffic to technologies that can be lawfully monitored. In some countries, regulations prohibit VoIP as a way to preserve income for national phone carriers. Allot SmartSentinel meets all of these challenges by leveraging world-class, DPI-powered traffic management on carrier grade platforms, to benefit both CSPs and governments

Key Benefits

- Gain full awareness of VoIP traffic in the network
- Enforce policies and regulations that block illegal VoIP usage
- Recover lost revenue from international and inbound roaming voice traffic

In Action

- Gain detailed visibility into VoIP traffic
- Overcome evasive tactics through Machine Learning powered DPI
- Prevent VoIP based fraud by blocking illegal VoIP voice traffic
- Degrade or block criminal and terrorist VoIP traffic to divert it to channels that can be monitored

Powered by

- Service Gateway
- NetXplorer
- SMP
- ClearSee

Departments

Security/Operations

Technology

Fixed, Mobile, Converged

Key Benefits

- Enforce safe internet regulations
- Protect citizens from malicious content
- Support millions of users without impacting network performance

Blacklist Web Filtering In Action

- Integrate with authorized blacklists such as Internet Watch Foundation (IWF)
- Automated blacklist updates ensure constant policy enforcement
- Easily integrate additional blacklists (provided by the government or any trusted source)
- Website categorization engine enables comprehensive and sophisticated filtering

Powered by

- Service Gateway
- NetXplorer
- ClearSee

Departments

Telecom Regulators/
Law Enforcement

Technology

Fixed, Mobile, Converged

FILTERING OF ABUSIVE WEB CONTENT

Government regulators seek to block access to illegal or harmful content. Allot's SmartSentinel delivers a carrier grade web filtering service that gives you the flexibility to proactively ensure a safer and more protected Internet environment for your country. With the power to inspect all traffic on country-wide networks, SmartSentinel's web filtering capabilities ensure that blacklisted and illegal Internet sites are blocked in real time.

CONTROL OF LIVE STREAMING VIDEO BROADCASTS

Live streaming of video broadcasts has catalyzed crowd-sourced news and enables real-time reporting through social networks and applications. However, it also allows offensive content to be distributed without any supervision. Moreover, even the tech companies that own and operate the live stream platforms are unable to react on time to stop harmful videos from proliferating worldwide. Terrorists use these platforms to broadcast horrific videos in real-time; rioters spread inciteful footage that fuels further unrest; and people committing suicide encourage unstable teens, and others, to follow suit. Governments need the ability to react in real time and legally block dangerous live videos to prevent potentially harmful consequences.

Key Benefits

- Prevent broadcasts of harmful videos
- Protect your citizens from viewing violent and abusive footage
- Deny terrorist, extremists, and abusive offenders from distributing illegal live content

In Action

- Identify uploads of popular live video services like Facebook Live and YouTube Live and block them if necessary
- Detect viewing of live video broadcasts and stop them when required
- Blocking can be limited by location to prevent network-wide shutdown of live broadcast services
- Identify creators of illegal live videos (depending on coverage)

Powered by

- Service Gateway
- NetXplorer
- ClearSee

Departments

Telecom Regulators/
Law Enforcement

Technology

Fixed, Mobile, Converged

Key Benefits

- Total network visibility enables recording of every data session
- Unlimited storage supports retention for long periods of time
- Built-in reporting and retrieval interfaces for querying retained information
- Optional export of stored information to external 3rd party systems

In Action

- Obtain granular, big data visibility into user sessions through high-end DPI classification engine, enabling subscriber usage identification
- Retention of detailed data records that include applications used, websites visited, subscriber location and more
- Powerful data warehousing supports retention for as long as required by law
- Integrated analytics and reporting allows investigating the stored information

Powered by

Service Gateway

NetXplorer

ClearSee

Data Mediator

Departments

Telecom Regulators/
Law Enforcement

Technology

Fixed, Mobile, Converged

DATA RECORDS RETENTION AND RETRIEVAL FOR LAW ENFORCEMENT AGENCIES

Criminals have massively transitioned to internet-based communications to avoid lawful monitoring and surveillance. This has led to a corresponding growth in Law Enforcement Agency (LEA) requirements for massive retention of internet and data usage records. These records are stored for long periods of time – months or years – and are used to assist the LEAs with investigations and intelligence research.

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, contact digital.enforcement@allot.com

allot