allot
See. Control. Secure.

Allot SmartSentinel
The Regulatory Compliance Solution for CSPs

Introduction

Regulatory compliance has become mission critical for Communication Service Providers (CSPs) due to increased cyber threats such as offensive, criminal, or unethical online activities, and attacks on communications infrastructure. Regulations aimed at protecting the general population require network operators to block harmful content and sites, safeguard communications infrastructure against denial of service attacks, and 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 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.

Benefits

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

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

Solution

The Allot SmartSentinel solution is specifically designed to enable CSPs to meet national law enforcement and/or homeland security authority requirements.

Flexible Deployment

SmartSentinel can be deployed in-line for active mitigation and filtering, or as a passive probe to monitor live traffic. It is suited to any network type; fixed or mobile, any network technology, and any deployment mode. The solution presents a centralized management platform to deploy action policies across the entire network at a national scale, and includes steering and chaining capabilities to easily integrate 3rd party products for enhanced solutions.

All Allot solutions support on-premise, cloud, hybrid, and virtual deployments.

Use Cases

SmartSentinel supports the following main Use Cases:

SECURITY

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

NETWORK INTELLIGENCE

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

APPLICATION & CONTENT FILTERING

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

QoE MONITORING & ENFORCEMENT

- QoE measurement supporting multidimensional KPIs from network, through subsystems, to subscriber-level
- Sophisticated traffic shaping allowing enforcement of QoE regulations
- Advanced Machine Learning and AI that enable powerful analytics, to pinpoint root cause of degraded QoE quickly and efficiently

VoIP MANAGEMENT

- Cutting-edge VoIP signature engine that detects all VoIP applications
- ML/DL driven heuristics that detect VOIP traffic that was encapsulated in other traffic in an attempt to avoid detection
- Blocking VoIP traffic to allow reclaiming lost revenue and provide high ROI

DATA RETENTION

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

High Performance and Scale

Allot's unified SmartSentinel solution can scale to inspect terabits per second (Tbps) of data and store petabytes of application and user data.

July 2020