
allot
See. Control. Secure.
ALLOT
DIGITAL SOVEREIGNTY
PLATFORM

WHAT IS

DIGITAL SOVEREIGNTY?

Achieving Digital Sovereignty requires governments to continuously safeguard their national digital infrastructure and data through Network Visibility and Protection. However, the exponential growth of harmful online content, rapid changes in user behavior, and the increase in VPN and anonymizer use for illegal online activity make this difficult.

OUR SOLUTION

ALLOT DIGITAL SOVEREIGNTY

The Allot solution for digital sovereignty is deployed inline in the network, using DPI technology which operates 24/7 to analyze 100% of network traffic. It sees all network traffic at a national, regional and subscriber level, controls internet, URL activity, VPNs and applications, including social media activities, and secures and protects strategic assets and national infrastructure from cyberattacks.

ALLOT DIGITAL SOVEREIGNTY

FEATURES

The Allot Digital Sovereignty solution offers the following features which can integrate to deliver a comprehensive digital sovereignty environment:

Web Filtering

Blocks illegal or prohibited HTTP and HTTPS URLs and domains, at national, regional and subscriber level based on a user-defined blocklist of websites or categories. Connections can be redirected, leading subscribers to a landing page informing them that they are trying to access illegal or prohibited websites. Integration with IWF and other external databases can also be provided.

Application Classification & Control

IP traffic classification and policy-based control at national, regional and subscriber level using DPI signatures for several thousand applications and sub-applications (e.g., WhatsApp text, YouTube Live upload, Facebook Messenger, Signal VoIP, Twitter). The application classification, alongside other parameters such as subscriber ID, time of day, data consumption, etc. is then used to manage national IP traffic bandwidth by blocking, throttling or prioritization of specific applications or services.

Location-based Enforcement (LBE)

Cross mobile-network enforcement based on geographical target areas, designed to support location-based enforcement use cases such as sterile area management.

VPN Classification & Control

Detection and control of all VPN services at national, regional and subscriber level. Identification, traffic classification and control of different anonymizers such as TOR, Psiphon and Opera including full blocking of the selected VPN, using special machine learning algorithms.

DDoS Protection

Acting as country's first line of defense, provides three key protection vectors at the national level: Infrastructure protection (Networks), Host weaponization prevention (Users/Devices/IoT), and Service protection (QoE, QoS and VAS). DDoS protection is based on two separate technologies: Network Behavior Anomaly Detection (NBAD), against DDoS attacks, and Host Behavior Anomaly Detection (HBAD), against botnet behavior.

Network Visibility and Analytics

Using DPI technology, provides complete detailed network visibility and storage of mass national data traffic (metadata) from network protocols and applications, down to the subscriber device and location level. Real-time analytics for national network and subscriber usage, with user-customized reports.

ALLOT DIGITAL SOVEREIGNTY

USE CASES

The Allot Digital Sovereignty solution is a versatile platform. It gives governmental organizations the ability to address a long list of challenges that they face on a daily basis. It enables them to operate on a National, Regional and individual Subscriber level. In addition, the solution can manage valuable monetization scenarios that can generate revenue for the country/government. Following are some of the primary examples of these scenarios.

NATIONAL LEVEL

NATIONAL DIGITAL REGULATION

VoIP Management

Block Voice over IP (VoIP) traffic if it does not comply with national regulations. Using Application Control and Reporting tools, the relevant agency can have stronger control over communication channels in their country to encourage more traditional telecom methods of communication, which are easier to investigate in case a crime is committed.

VPN Management

Using VPN Management tools, governments can see the types of traffic that end users access on the internet. Virtual Private Networks (VPNs) have become quite popular over the last number of years, enabling users to hide their data traffic and identity, thereby avoiding the scrutiny of the regulator. The Allot solution helps regulators see many popular VPNs.

Digital Monetization

The Allot solution enables government agencies to regulate certain online services and generate license fees/tax for content providers that want to open their services in the country. Examples of online services can be gambling activities, cryptocurrency transactions or any other online activities that the government would like to regulate and monetize in the country.

Fraud Management

Governments can use digital methods to combat fraudulent transactions online and avoid traffic leakage in the country. These, and similar scenarios are enabled through URL Filtering, Application Control and the Reporting capability of the Allot platform.

Operator's Operation Inspection

Government regulators need to keep tabs on telecom operators' and ISPs' operations to ensure that they comply with communications regulations. Using Bandwidth Management and Reporting Tools, over 100 countries currently use the Allot solution to ensure active compliance to agreed-upon bandwidth usage standards.

NATIONAL DIGITAL ENFORCEMENT

Illegal or Harmful Content Prevention / Dangerous Content Blocking

Government enforcement agencies seek to block access to illegal or harmful content and stop the propagation of damaging fake news. Allot's solution delivers carrier grade Web Filtering, Application and VPN Visibility and Control services to governments worldwide that provide the flexibility to proactively ensure a safer and more protected national internet environment.

Emergency 'Red Button'

Application Control enables a country to quickly and easily block or throttle bandwidth for an application or a subservice of an application (e.g., block WhatsApp completely or WhatsApp video calls only).

Instant Messaging CDR Management

Instant Messaging (IM) platforms have been progressively replacing traditional telephony systems for multiple reasons: They support text, audio, video and file transfer, they give communication privacy to the users with end-to-end encryption and they are free on top of the internet connection. The Allot solution enables identifying and matching the users of Instant Messaging Applications for voice and video calls in the networks, for regulatory or law enforcement.

NATIONAL FIREWALL

DDoS Protection

Implemented worldwide, Allot inline DPI-based DDoS protection, using Network Behavior Anomaly Detection (NBAD) technology, enables complete traffic captures without aggregation or sampling, for granular and detailed information leading to faster and more accurate attack detection. The advantages of DPI-based mitigation include its ability to dynamically filter out attack traffic without impacting legitimate traffic, as well as providing quality forensics for real-time and post-attack analysis, all with significantly low Time-to-Response.

Botnet Protection

Using Host Behavior Anomaly Detection (HBAD) technology, Allot inline DPI-based botnet protection enables identifying abusive activity generated by compromised IoT and bot-infected endpoints and can block access to C&C servers to make the botnet devices inoperative.

Threat Protection for Governmental Infrastructure

Allot can protect governmental network infrastructure and government employees against online phishing, malware, spyware, and ransomware sites by using its state-of-the-art network-native, zero-touch Allot Secure solution.

REGIONAL LEVEL

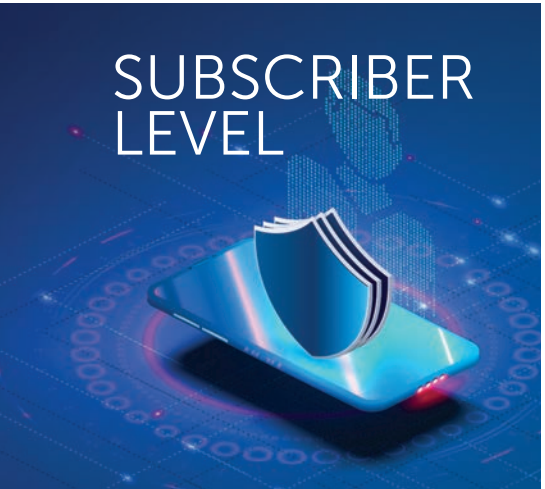
Sterile Area Management

In public events scenarios such as VIP visits, an agency can use Application Control, the Subscriber Management Platform (SMP) and Location-based Enforcement (LBE) to temporarily block all or some of the social media networks and / or instant messaging apps in a defined geographical area, for all or a subset of subscribers, to protect high-value individuals from harm and avoid situation escalations. In addition, within the defined area, the authorities can protect bandwidth for government/ security use to ensure their ability to securely communicate during an event.

Crisis Management

When quick action is required, for example, when a peaceful demonstration starts to turn into a riot, authorities can use Application Control and Location Based Enforcement tools to manage the spread of incitement on social networks by temporarily blocking or limiting specific services, applications or application features.

SUBSCRIBER LEVEL



Forensic investigation

Law enforcement agencies use Network Visibility and Analytics tools to collect raw data about subscriber usage and learn patterns of online usage and act accordingly.

ABOUT ALLOT

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a leading global provider of innovative network intelligence and converged security solutions for service providers, enterprises and governments worldwide. Allot solutions are deployed globally for network and application analytics, traffic control and shaping, network-native security services, and more. Allot's multi-service platforms are deployed in more than 100 countries by over 500 mobile, fixed and cloud service providers, including 5 of the top 10 communications service providers, and over 1,000 enterprises. The Allot industry-leading network-native security-as-a-service solution is used by many millions of subscribers globally. Allot has more than 25 years of deployment experience, serving more than one billion subscribers in total, and offers 24/7 follow-the-sun support.

For more information contact us or click here to learn more.