# Allot IoTSecure

## Addressing Communication Service Provider Challenges Related to the Internet of Things

White Paper

See. Control. Secure.

# Contents

# Allot IoTSecure

Addressing Communication Service Provider Challenges Related to the Internet of Things

## 1 Why We Should Be Worried about IoT

The Internet of Things (IoT) has found its way into many aspects of our lives and businesses, and is prevalent in almost all types of national critical infrastructure. IoT has also become the target of malicious criminal and state-sponsored activity. The need to secure IoT and ensure continuity of IoT based services is a reality recently demonstrated when DDoS attacks left Finland housing without heating.

Vulnerable connected devices have also changed the DDoS threat landscape, as witnessed in the DDoS attacks on Krebs and Dyn in late 2016. The sheer volume of DDoS traffic had an impact not only on the intended victims, but also on the communications infrastructure it traversed.

As has been widely publicized by many security researchers, the vulnerability of some IoT devices borders on negligence[1,2]. Some of these devices are impossible to patch or incorporate with third party security software. According to Gartner this situation will get worse over time with total IoT endpoint shipments outpacing the rate of securing those endpoints[3].

The sorry state of IoT security coupled with the lack of visibility of IoT behavior has the following impact on Communication Service Providers (CSPs) and mobile operators.

- Security concerns remain the number one reason why Enterprises are hesitant about deploying IoT services. CSPs that are quick to provide value-added services that address cyber threats will gain a competitive advantage.
- Operational efficiency will become impaired. For example, mobile operators have sold IoT SIMs in bulk without any knowledge of the type of service deployed. This lack of visibility disrupts planning and troubleshooting capabilities in addition to interfering with data package management against fraudulent or innocent misuse.
- CSP infrastructure must be protected against both large internal and external volumetric IoT DDoS attacks.

[1] http://www.zdnet.com/article/history-repeating-how-the-internet-of-things-failed-to-learn-the-security-lessons-of-the-past/

[2] https://www.ftc.gov/news-events/blogs/business-blog/2017/01/d-link-case-alleges-inadequate-internet-things-security

[3] Forecast: IoT Security, Worldwide, 2016; Published: 7 April 2016 ID: G00302108 - Analyst(s): Ruggero Contu, Peter Middleton, Earl Perkins, L Akshay

**Allot IoTSecure** Is designed to tackle these challenges with the following benefits:

- Create new IoT Value Added Services to increase monetization
- Increased operational efficiency
- Addressing of Enterprise security concerns
- Protection of CSP communications infrastructure

# 2 Allot IoTSecure


**Figure 1. Allot IoTSecure**

Allot IoTSecure brings to bear proven capabilities in carrier-class security, behavior analysis, and traffic intelligence and control. The solution is comprised of the following elements:

- Behavior Assurance
- Behavior Profiling
- IoT Security

An IoT device is designed for a specific purpose. Unlike a smartphone, its behavior can be expressed—with whom it communicates, how much data it generates and receives, what protocols it uses, and even time-of-day or day-of-the-week dependencies. This provides the basis for the first two elements of the solution—**Behavior Assurance**, and **Behavior Profiling**.

**Behavior Assurance** is the ability to define a policy that provides specific traffic parameters based on known behavior of the IoT deployment. By whitelisting the known parameters, such as who the devices communicate with and what protocols and applications should be used, the attack surface is significantly reduced. Unfortunately, not all parameters are known by the Enterprise in advance, and in the case of consumer IoT, these may be limited or non-existent.

**Behavior Profiling** is based on a machine-learning process that is applied to each individual IoT device, such as surveillance cameras, electricity meters, vending machines, and telemetry devices, each of which exhibits individual behavior.
The immediate benefit is that the operator can see clearly the types of devices deployed on the network. IoTSecure builds a baseline of multiple traffic parameters such as data rates, numbers of connections, and rates of connection establishment to identify anomalous behavior. Deviations from the individual or group baseline identifies a compromised, malfunctioning, or infected device, or it will warn upon fraud detection and data plan misuse.

The third element, **IoT Security,** is a network-based security solution that is device agnostic. Its multilayer approach addresses pre-infection and post-infection scenarios and provides the following functions:

- Carrier-class, network-based anti-malware that protects against IoT malware such as Mirai and IOTroop through partnerships with industry leading anti-virus engines.
- Bot identification and mitigation based on analysis of device behavior to identify Bot activity patterns and filtering of Command & Control servers and other malicious web sites.
- Bi-Directional DDoS detection and mitigation protects an IoT service from attacks that arrive from external networks and stops DDoS attacks from IoT devices connected to the Service Provider infrastructure.

To facilitate remote remediation and still contain an infected device, a **smart quarantine** policy can be applied that limits communications, enabling only maintenance and remediation systems to access the suspect device.

# 3 Benefits of IoTSecure

This solution provides many benefits and use cases that can be grouped into two categories—improved **Operational Efficiencies** and **IoT Value Added Services**, which enhance IoT monetization.

## 3.1 Operational Efficiency

Operational efficiency is key to scaling and protecting the communications infrastructure efficiently and support the rapid growth of IoT and related infrastructure investments. IoTSecure provides the ability to make informed investment decisions, expedite troubleshooting, and verify that customers meet the terms and conditions of an IoT Data Plan.

### 3.1.1 IoT Visibility

Data collection, analytics, and behavior analysis are the key components of IoTSecure. Allot's DPI platform delivers carrier-class data collection by inspecting every packet and identifying devices, traffic flows, network utilization, and application/protocol usage.

Utilizing an HP Vertica big data repository and MicroStrategy business intelligence for scalable, real time and historical analytics, and event reporting, IoTSecure Analytics increases operational efficiency by supporting:

- Behavioral analysis and anomaly detection
- Trend analysis and capacity planning
- Data-driven decisions for informed troubleshooting
- Policy definition for network optimization and QoS enforcement

It can also serve as a data source, providing raw or correlated data for external analytical solutions.

Visibility and behavioral analysis of IoT can also be used to flag the misuse of data plans. We have already deployed this capability in a Tier-1 operator who was concerned about SIMs installed in electricity meters finding their way into laptops or smartphones.

### 3.1.2 IoT Infrastructure Protection

IoTSecure ensures resilience of the CSP infrastructure and maintains QoE for customers that rely on the 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 DDoS detection
- Bi-directional detection and mitigation.
- Detection and mitigation under a minute.
- QoE-based congestion control
- Session awareness

Together, these features protect the infrastructure against DDoS attacks initiated from internal and external sources and maintain the QoE of bystanders sharing the same network. Allot DDoS mitigation solutions are deployed today in carrier networks, protecting Terabit infrastructure at the national level.

IoTSecure bot detection can also provide a proactive indication of compromised deployments in a CSP network that has the potential of launching a DDoS attack.

## 3.2 IoT Value Added Services

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 capabilities as additional assets to their connectivity services to increase IoT monetization and differentiate their offering for an additional competitive advantage. IoT Value Added Services would be provisioned by the operator, or through a customer self-care portal.

IoT network based Value Added Services are fully aligned with the operator's expertise and core business.

These services can be offered in tiers, for example:

- IoT Security
- IoT Behavior Assurance
- IoT Behavior Profiling and Anomaly Detection

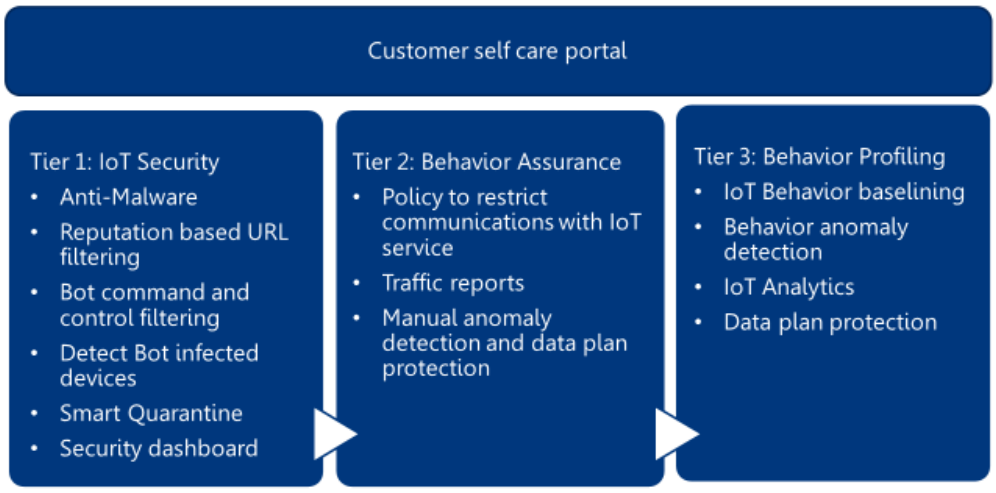


**Figure 2. Tiered Value-Added Services**

## 3.2.1 IoT Security

Mirai hit the headlines in 2016, but its code was publicly available before the attack on Dyn and many commercially available anti-viruses already held signatures to block it. The problem was that IoT devices are difficult or impossible to patch and are typically unable to run client software intended to protect these devices.

### Prevent IoT Device Infection

IoTSecure provides network-based **anti-malware** in a carrier-class solution and is field proven today protecting millions of mobile devices. Incoming traffic is inspected by using leading AV engines—McAfee, Kaspersky, Bit Defender, and/or Sophos. A network-based solution is the only effective way to prevent infection of IoT devices.

### Identifying and Handling Infected IoT Devices

IoTSecure employs two **anti-bot** mechanisms. The first is a tried and proven network-based Host Behavior Anomaly Detection (HBAD) engine that matches traffic patterns to specific types of bot activity. The second layer is based on **filtering of bot Command & Control servers**. Bots that are unable to communicate with their C&C servers are typically rendered useless.

This multilayer approach provides quick and accurate identification of infected IoT devices. To contain an infected device, IoTSecure provides a **Smart Quarantine** function that limits the traffic from those devices to a minimal bandwidth, and provides access only to maintenance systems that are crucial for remote devices that are not readily accessible to a technician.

### 3.2.2 Behavior Assurance

An IoT service typically delivers a specific or a limited set of functions, and communicates directly with a limited set of management servers and services. Behavior assurance policies limit the IoT communications by source, destination, application and protocol to reduce the attack surface of the device. For example, a Point-of-Sale (POS) device should communicate with a financial transaction server and a management server, and communication with any other destination would be blocked by the network. IoTSecure provides granular access control and traffic policing on a large scale—as proven, and deployed globally in carrier networks and datacenters—and has the scale and robustness to police the largest of IoT deployments.

The policies can be defined in the following terms:

- Source and Destination address or domain of the servers authorized to communicate with the IoT devices
- APN
- IMEI
- Type of protocols and applications permitted for communication
- Time of day/day of week for when the communication is permitted
- Number of new connections and amount of bandwidth permitted for the communication
- Location

These policies are useful for reducing the attack surface and limiting the ability of attackers to take control of the IoT devices.

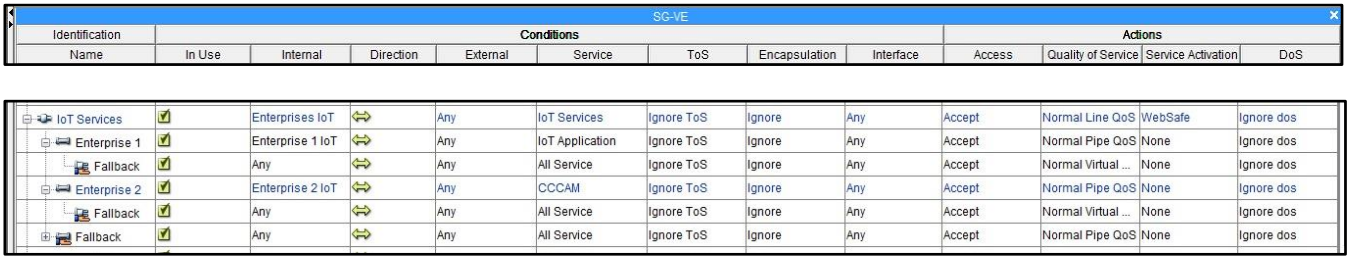


**Figure 3. Allot's Policy Editor to Control IoT Traffic**

### 3.2.3 IoT Analytics and Behavior Profiling

Just as IoT analytics is key to operational efficiency for the CSP, providing the same granular analytics to an enterprise would add tremendous value for them to manage and maintain their IoT deployments. Today, visibility is provided at the control plane and it is very limited. Providing the full stack of network and traffic analytics provides enterprise IoT engineering and operations with a deeper analysis of device behavior for troubleshooting, security incident management and design improvements. IoT analytics is also the basis for IoT behavior profiling and anomaly detection. IoTSecure builds a profile for each device and groups of similar devices.

### 3.2.4 Data Plan Protection

In many cases IoT data plans are grouped with one quota covering hundreds of devices that typically consume small amounts of bandwidth. Through behavior profiling, IoTSecure flags devices that are generating a large amount of traffic compared to the average of the group, either due to malfunction, infection, or due to SIM misuse. Identifying these devices in real time and alerting the customer to avoid bill shock or traffic throttling for the entire group of devices will help avoid customer dissatisfaction and contention.

# 4 The IoT Ecosystem

Integration with IoT platforms and mobile infrastructure is a key component of the solution. This includes:

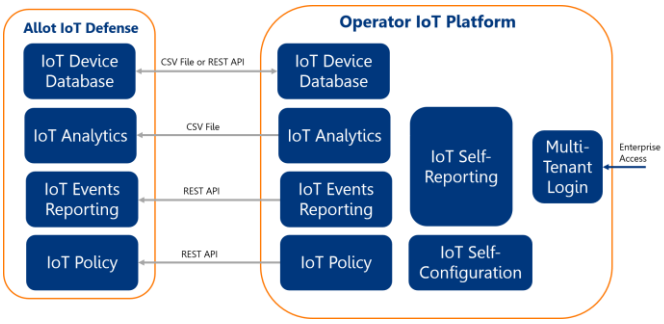


Figure 4. IoT Ecosystem

- Mobile IoT platforms that host the IoT database and policy and consolidate IoT analytics and reports. This may also include the IoT mobile identity systems that help correlate device IMSI (device telephone number), IP addresses, and customer identity.
- Third party IoT connectivity management platforms that provide network usage, geo-location, and health status related to IoT mobile connectivity.
- Multi-tenant customer management capabilities served via an API.

# 5 Summary

**IoTSecure** is based on the existing capabilities of Allot's multiservice platforms, which are deployed on hundreds of CSP networks around the globe. They provide Allot's three pillars—**visibility**, **security**, and **control**—that are required to ensure service availability for IoT deployments and protect IoT infrastructure when, and if, the "things" misbehave.

**Behavior Assurance**, **Behavior Profiling and Anomaly Detection**, and **IoT Security** (anti-bot, anti-malware, and DDoS protection), provide a scalable approach to dealing with the challenges of IoT deployments. This enables CSPs to increase operational efficiency and extend their portfolio of value-added services for incremental revenue and increased customer satisfaction.

P/N Dxxxxxx Rev.1

**www.allot.com sales@allot.com**

**Americas**: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA - Tel: +1 781-939-9300; Fax: +1 781-939-9393; Toll free: +1 877-255-6826

**Europe**: NCI–Les Centres d'Affaires Village d'Entreprises, 'Green Side' 400 Avenue Roumanille, BP309 06906 Sophia Antipolis, Cedex France - Tel: +33 (0) 4-93-001160; Fax: +33 (0) 4-93-001165

**Asia Pacific**: 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104, Tel: +65 6749-0213; Fax: +65 6848-1015

**Japan**: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 - Tel: +81 (3) 5297 7668; Fax: +81 (3) 5297 7669

**Middle East & Africa**: 22 Hanagar Street, Industrial Zone B, Hod Hasharon, 4501317 Israel - Tel: 972 (9) 761-9200; Fax: 972 (9) 744-3626