Cyber Security Intelligence & Threat Mitigation

Allot communications

Yaron Bielous
Head of Cloud

April 1st 2015

About Allot Communications
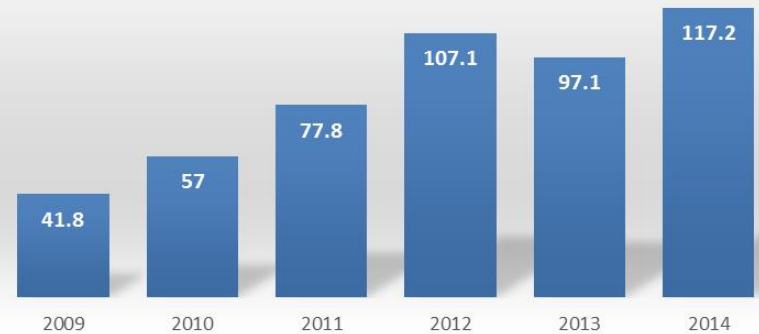

Founded in 1996

Traded on NASDAQ since 2006 – Symbol "ALLT"

4500+ enterprise and cloud customers

500+ fixed & mobile provider customers

Extensive partner ecosystem

Revenues in M$US

Year	Revenue
2009	41.8
2010	57
2011	77.8
2012	107.1
2013	97.1
2014	117.2

Global Presence - Selling in more than 100 countries

Enterprises migrated to Hybrid Cloud

Hybrid Cloud

Private Cloud

ORACLE
E-BUSINESS SUITE

E-COMMERCE

Public Cloud

salesforce · Dropbox for Business · f

Office 365 · webex · Linked in

94% of Respondents are Using Cloud

Public Cloud Only **29%** **58%** Public and Private **7%** Private Cloud Only
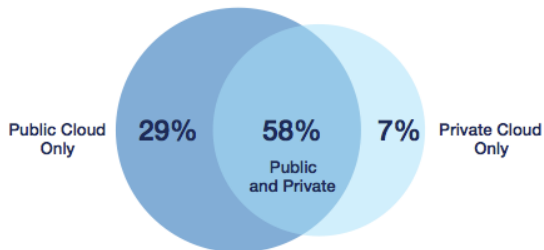
WAN

Internet

The Internet is the new IT

Ensuring Availability, Performance & Security across Clouds
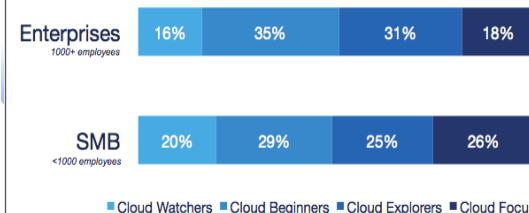
Users

On Campus

In the Branch

24/7

At Home

On the Road

B Y O D

Cloud Maturity Model by Company Size

	Cloud Watchers	Cloud Beginners	Cloud Explorers	Cloud Focused
Enterprises 1000+ employees	16%	35%	31%	18%
SMB <1000 employees	20%	29%	25%	26%

Source: RightScale 2014 State of the Cloud Report

Source: RightScale 2014 State of the Cloud Report

Allot's Solution Domains

Cloud Access Security

Threat Detection
DDoS Protection
Web Security

Cloud Access Optimization

Application Awareness
QoS
Policy Management
Traffic Steering

Engines

DPI Technology

P2P
Gold
Bronze
Silver
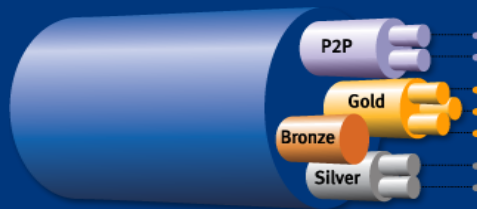
Network Traffic Analytics

Policy Control

Platforms

Allot Service Gateway   **Allot NetEnforcer**   **Allot NFV**

Allot
communications

4

Granular Web Analytics under encryption

Drill-down to Hosts and Apps is possible even when traffic is SSL encrypted
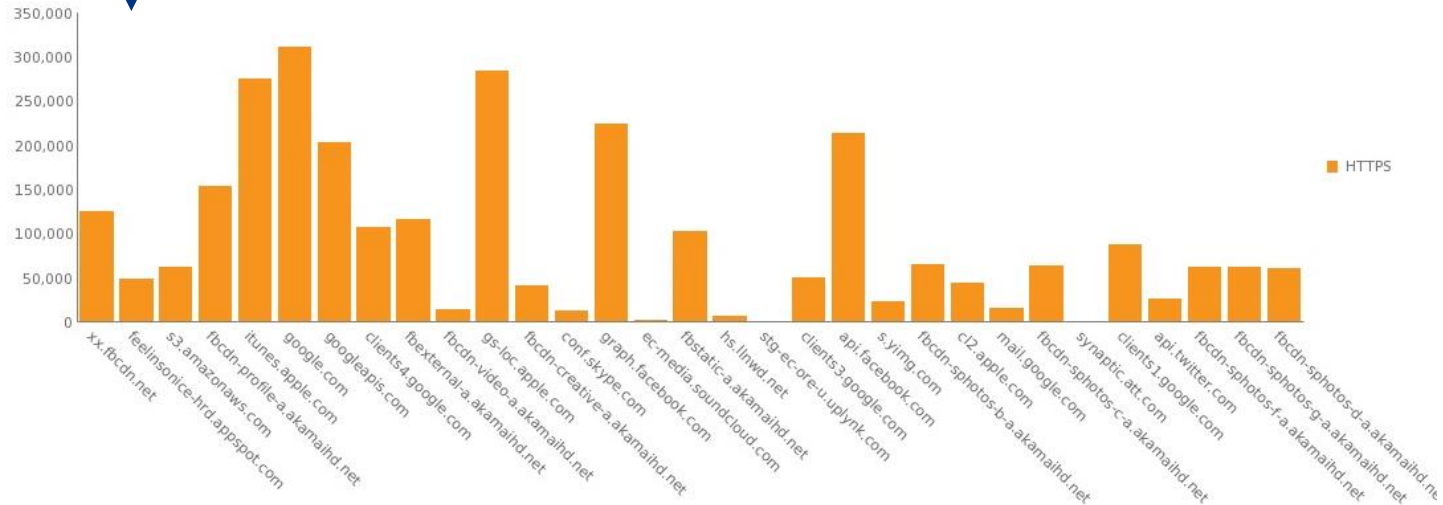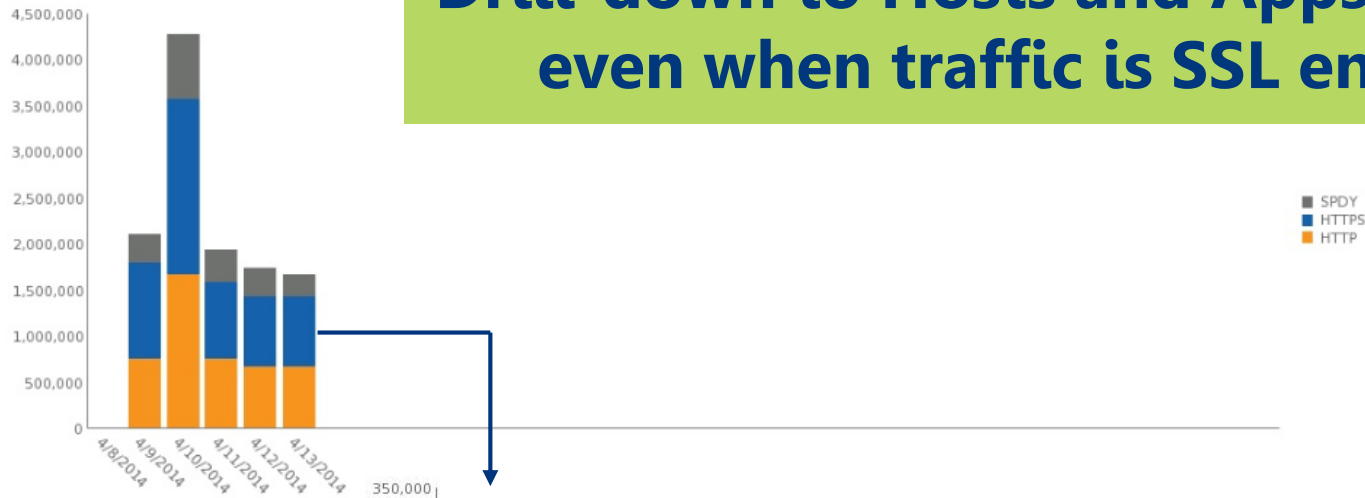
The Anonymity Risks

- May indicate illegal activity
- DDoS attacks behind anonymizes
- Hacking activity behind anonymizes
- Malicious activity detection under the anonymize shield is a significant challenge

Allot Value Proposition:
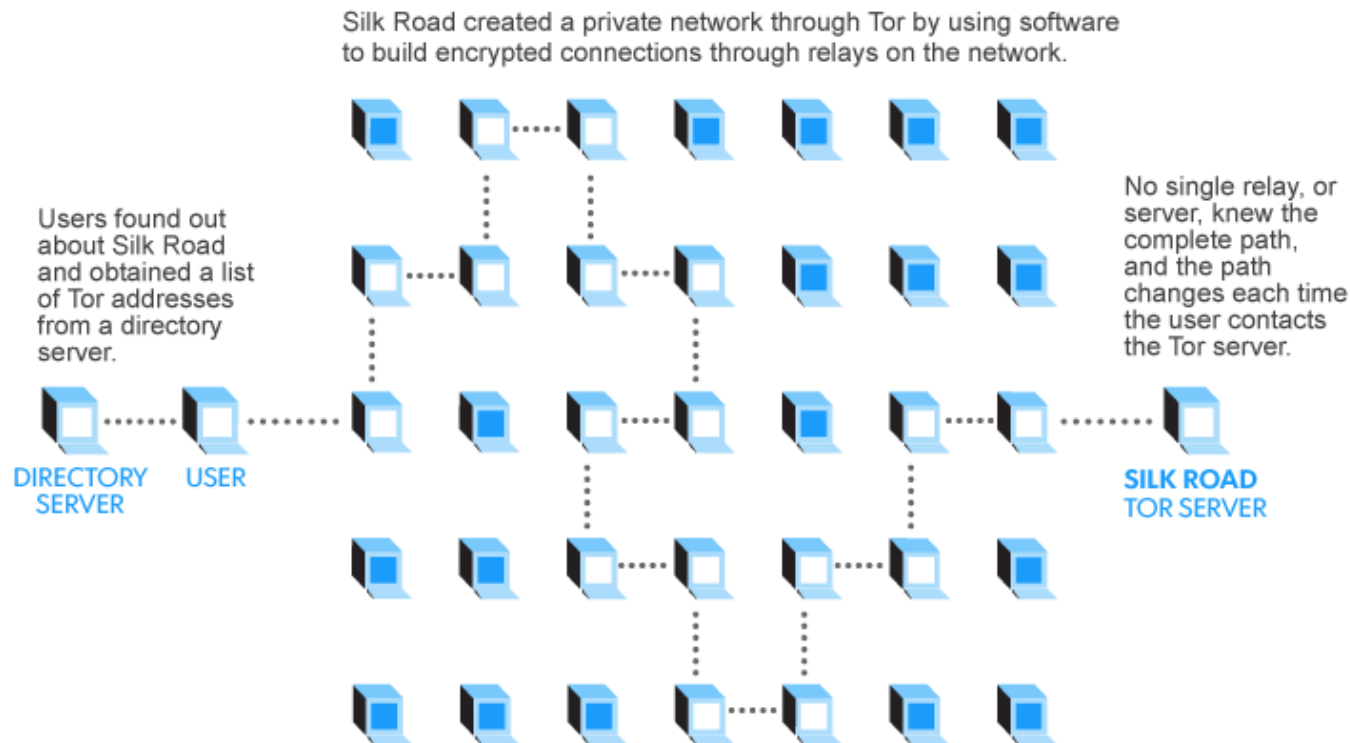**Delivers granular visibility into a wide range of anonymity tools**

Targeting Illegal Destinations
How FBI brought down cyber-underworld site Silk Road

SILK ROAD 101: HOW THE "DARKNET" WORKS.

Law enforcement officials shut down Silk Road, a sophisticated black market website offering illegal wares and services from heroin to hit men. The Silk Road website is located in the cyber underworld, also known as the "darknet."

TOR IS BASED ON AN "ONION ROUTING" SYSTEM DEVELOPED BY THE U.S. NAVY RESEARCH LAB TO HIDE MILITARY COMMUNICATIONS.

Silk Road created a private network through Tor by using software to build encrypted connections through relays on the network.

Users found out about Silk Road and obtained a list of Tor addresses from a directory server.

No single relay, or server, knew the complete path, and the path changes each time the user contacts the Tor server.

DIRECTORY SERVER   USER

SILK ROAD TOR SERVER

Richest Intelligence Directly from the Wire

Operations Intelligence

Control & Care

Security Intelligence

Experience Analytics

User Control

Regulatory Compliance

SIEM

Users
- On Campus
- In the Branch
- On the Road
- At Home

Mobile

Broadband

Applications

Private Cloud
- ORACLE E-BUSINESS SUITE
- E-COMMERCE

Public Cloud
- salesforce
- webex
- Dropbox for Business
- Office 365
- GoToMeeting

Internet
- Facebook
- Google
- Linked in

USER   LOCATION   ENDPOINT   NETWORK   CONTENT   APPLICATION

Allot communications

Proactive Web Intelligence
Indepth Analysis
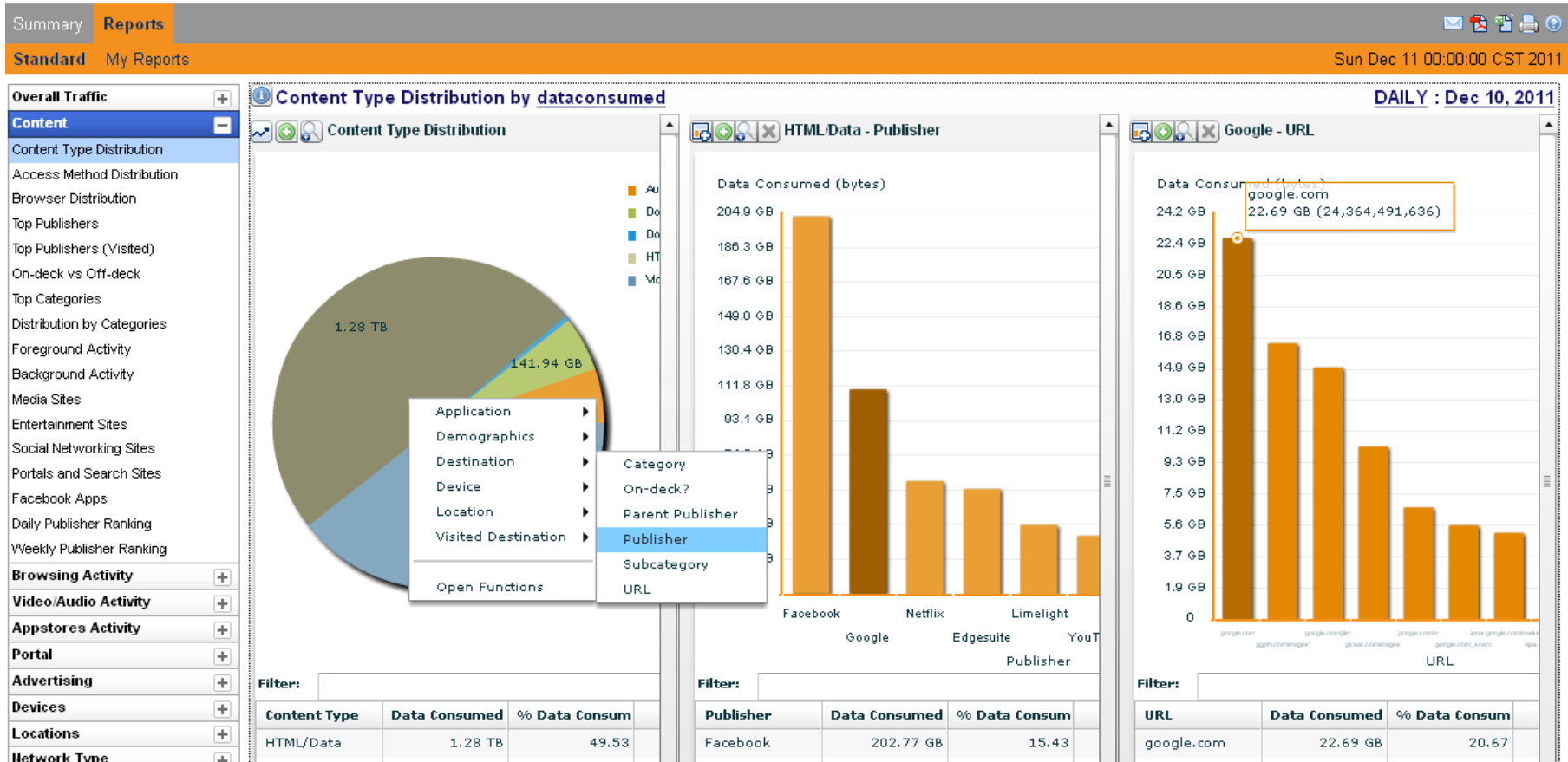
Individual User's Activity

Which application are used?
When? For how long?
On which device?

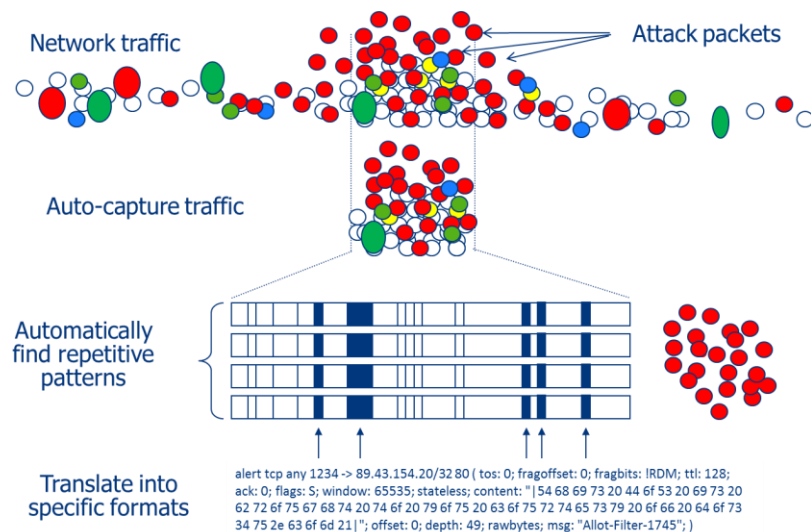# Actionable Security – DDoS Protection

NBAD Distribution for 2013-04-07 00:00 – 2013-04-09 00:00   Last refresh: 2013-04-08 00:45

Legend: Government | Business | Broadband | Mobile SP | Customers | ISPs | Others

DDoS/DoS/Scan attacks per Day

Network traffic

Attack packets

Auto-capture traffic

Automatically find repetitive patterns

Translate into specific formats

alert tcp any 1234 -> 89.43.154.20/32 80 (tos: 0; fragoffset: 0; fragbits: IRDM; ttl: 128; ack: 0; flags: S; window: 65535; stateless; content: "|54 68 69 73 20 44 6f 53 20 69 73 20 62 72 6f 6f 67 68 74 20 74 6f 20 79 6f 75 20 63 6f 75 72 74 65 73 79 20 6f 66 20 20 64 6f 73 34 75 2e 63 6f 6d 21|"; offset: 0; depth: 49; rawbytes; msg: "Allot-Filter-1745";)
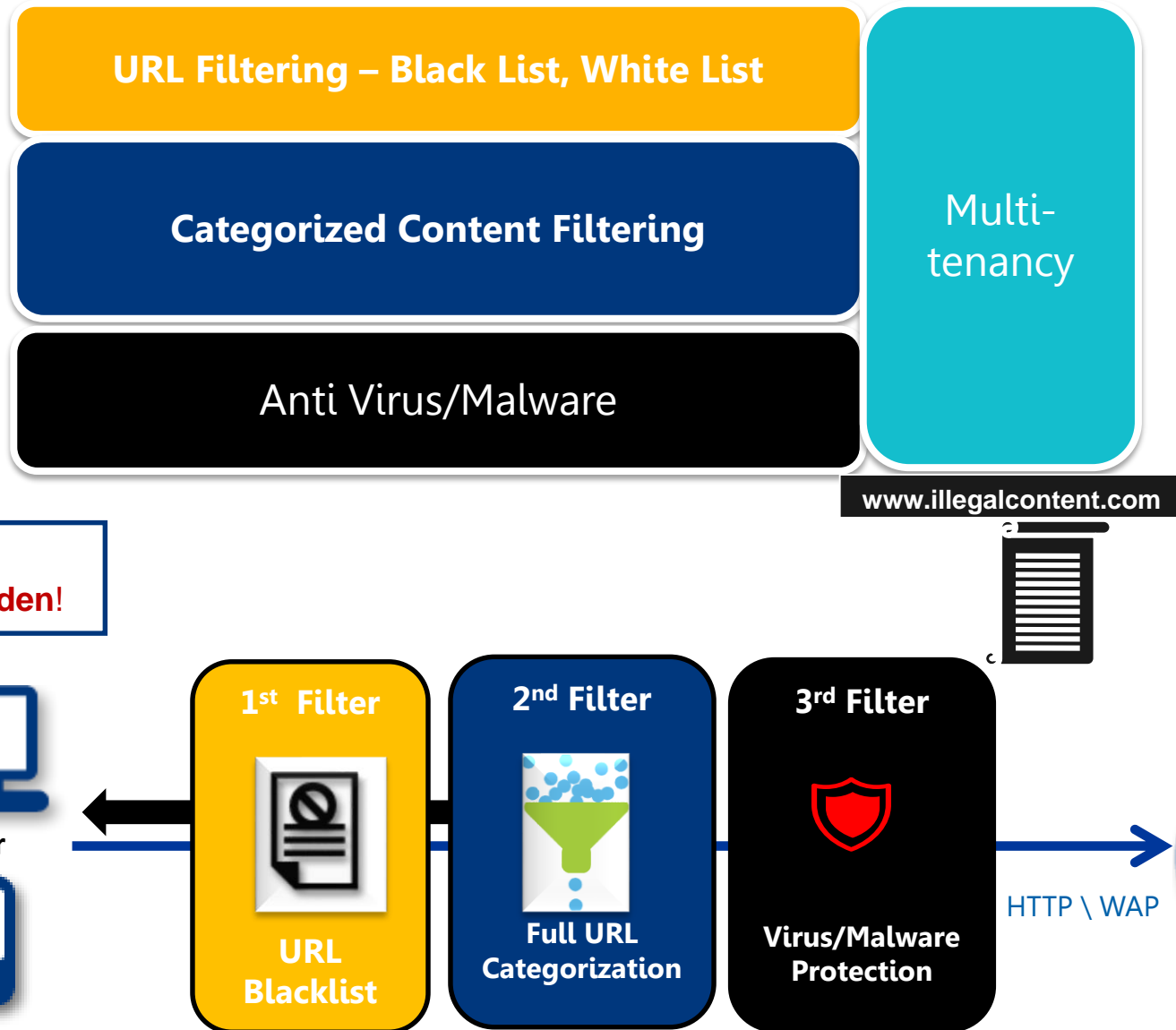
Anti-DDoS as a Service

Audit User Activity

Automatic/on-demand Mitigation action

11

Actionable Security – Web & Mail Protection

URL Filtering – Black List, White List

Categorized Content Filtering

Multi-tenancy

Anti Virus/Malware

www.illegalcontent.com

Access to this website is forbidden!

User

1st Filter
URL Blacklist

2nd Filter
Full URL Categorization

3rd Filter
Virus/Malware Protection

HTTP \ WAP

12

Allot Cyber Solutions for a Safer Internet

Cyber Intelligence

- Leading anonymity and encryption awareness
- Highly Granular Transaction information at Scale

Web Security

- Content filtering to illegal web services, and anti-malware protection

Network Protection

- Zero day DDoS Mitigation
- 1st line of defense

THANK Ü

Find out how Allot can help
YOUR business to become
a leading Digital Lifestyle Provider

Email info@allot.com
www.allot.com