Anti Bot For Aviation Industry

More Than Just Cloud

The Bot malicious Attack Increase Sharply in the world

AN AVERAGE DAY AT AN ENTERPRISE ORGANIZATION

SECONDS

EVERY 81 SECONDS
A known malware is downloaded

EVERY 4 MINUTES
A high-risk application is used

EVERY 4 SECONDS
An unknown malware is downloaded

EVERY 53 SECONDS
A bot communicates with its command and control center

EVERY 5 SECONDS
A host accesses a malicious website

EVERY 30 SECONDS
A threat emulation event occurs

EVERY 32 MINUTES
Sensitive data is sent outside the organization

1.1 SOURCE: Check Point Software Technologies

75%
of organizations had existing bot infections

82%
of organizations accessed a malicious site

88%
of organizations suffered a data loss incident

89%
of organizations downloaded a malicious file

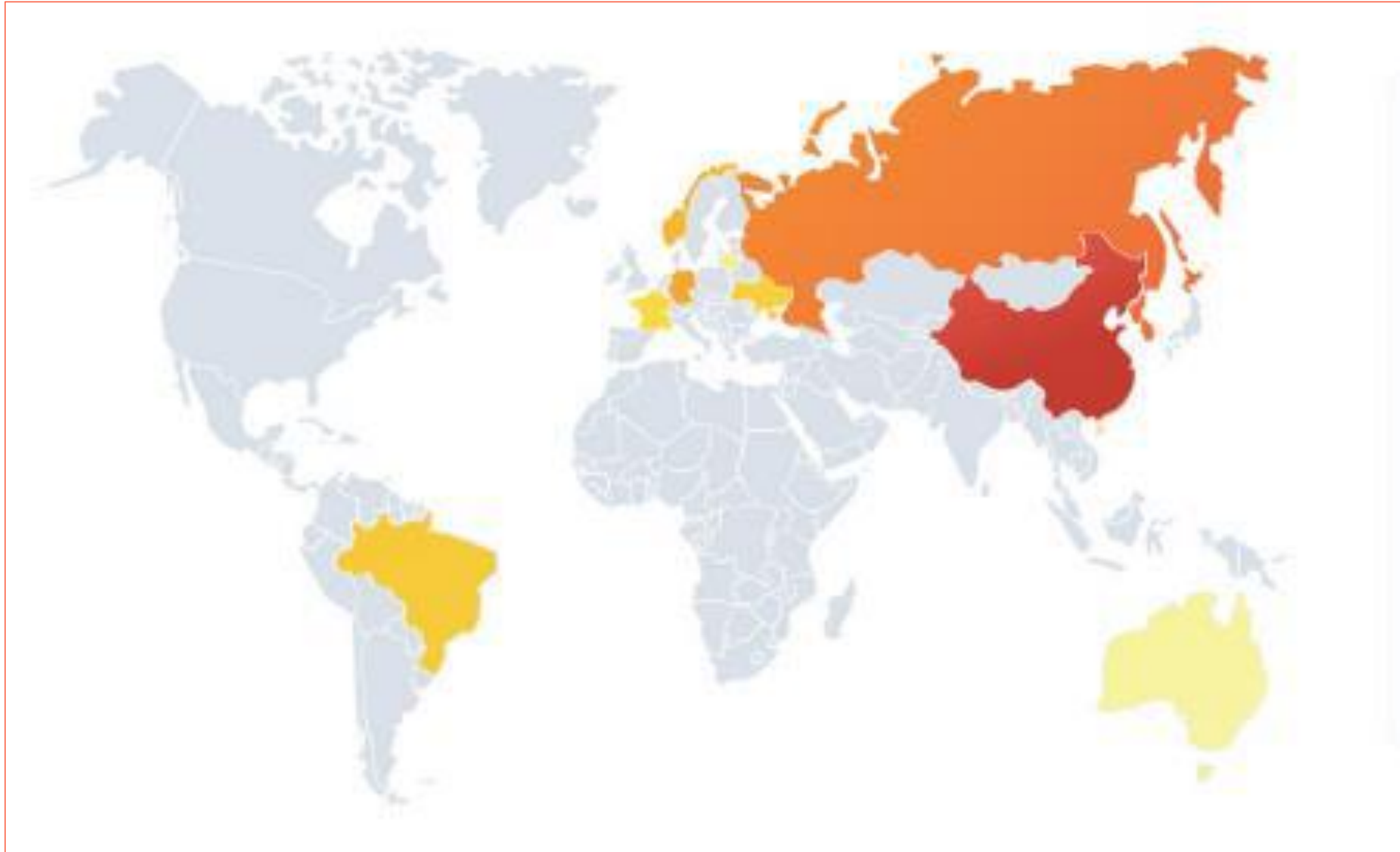Data Resource: Check Point 2017 Security Report

In 2016, a typical bot attempted to communicate with its command and control (C&C) server over **1,630** times per day, or once every **52.8** seconds. This speed and frequency continues to increase, jumping **12%** from the previous year, and **95%** more than in 2012.

While bot infection levels were down almost **10%** in 2016 from 2015, the numbers are still troubling. Almost **75%** of organizations studied were infected with bots in 2016, with **44%** of those active for more than four weeks.

The Global Bot malicious Attack Statistic

## The Thermodynamic Chart Of The Global Bot attack source

Data Resource: Check Point 2017 Security Report

- Over 75% attack coming from Greater China Region
- **German** is also typical bot attack source
- Top 3 industry which easily encounter the bot attack are **Aviation**, **E-commerce** and **Real Estate**

RECOGNIZED BOT ATTACKS TYPE

FAMILY	DAMAGE	PERCENT
SALITY	Steals sensitive information	18.6%
CONFICKER	Disables system security services, gains attacker remote access	18.6%
ZEROACCESS	Allows remote operations and malware download	6.7%
CUTWAIL	Spreads spam	5.1%
GAMARUE	Opens a backdoor for attacks	3.0%
ZEUS	Steals banking credentials	2.7%
LDPINCH	Steals sensitive information	2.1%
DELF	Steals authentication credentials	1.1%
RAMNIT	Steals banking credentials	1.0%
GRAFTOR	Downloads malicious files	0.9%

3 Top Industries attacked By Bot
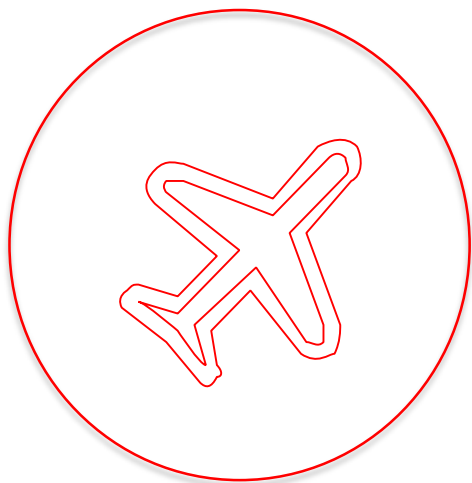
Aviation
- Ticket on-hold
- Low attendance rate
- Revenue loss

E-Commerce
- Product Price Crawler
- Product Lineup Crawler

Real Estate
- Real estate DB Crawler
- Competitor business analysis

More Than Just Cloud

Alibaba Cloud
Official Cloud Services Partner

The Aviation Industry Anti Bot Attack Scenario
AirAsia Anti Bot Case Study

AirAsia was under constant BOT attack overwhelming the backend servers resulted in significant expenses

AirAsia Berhad *is a Malaysian low-cost airline headquartered near Kuala Lumpur, Malaysia. It is the largest airline in Malaysia by fleet size and destinations. AirAsia Group operates scheduled domestic and international flights to more than 165 destinations spanning 25 countries.*

AirAsia *had more than* **50%** *of the global traffic flowing from China, when only less than* **10%** *of the total revenue was attributed to that traffic.*

Most of the traffic was either concentrated Bot attacks or hackers trying to scrap information from AirAsia websites trying to sell them in the Black Market.

Alibaba Cloud
Official Cloud Services Partner

The Aviation Industry Anti Bot Attack Scenario

AirAsia Anti Bot Case Study: Business Value Loss

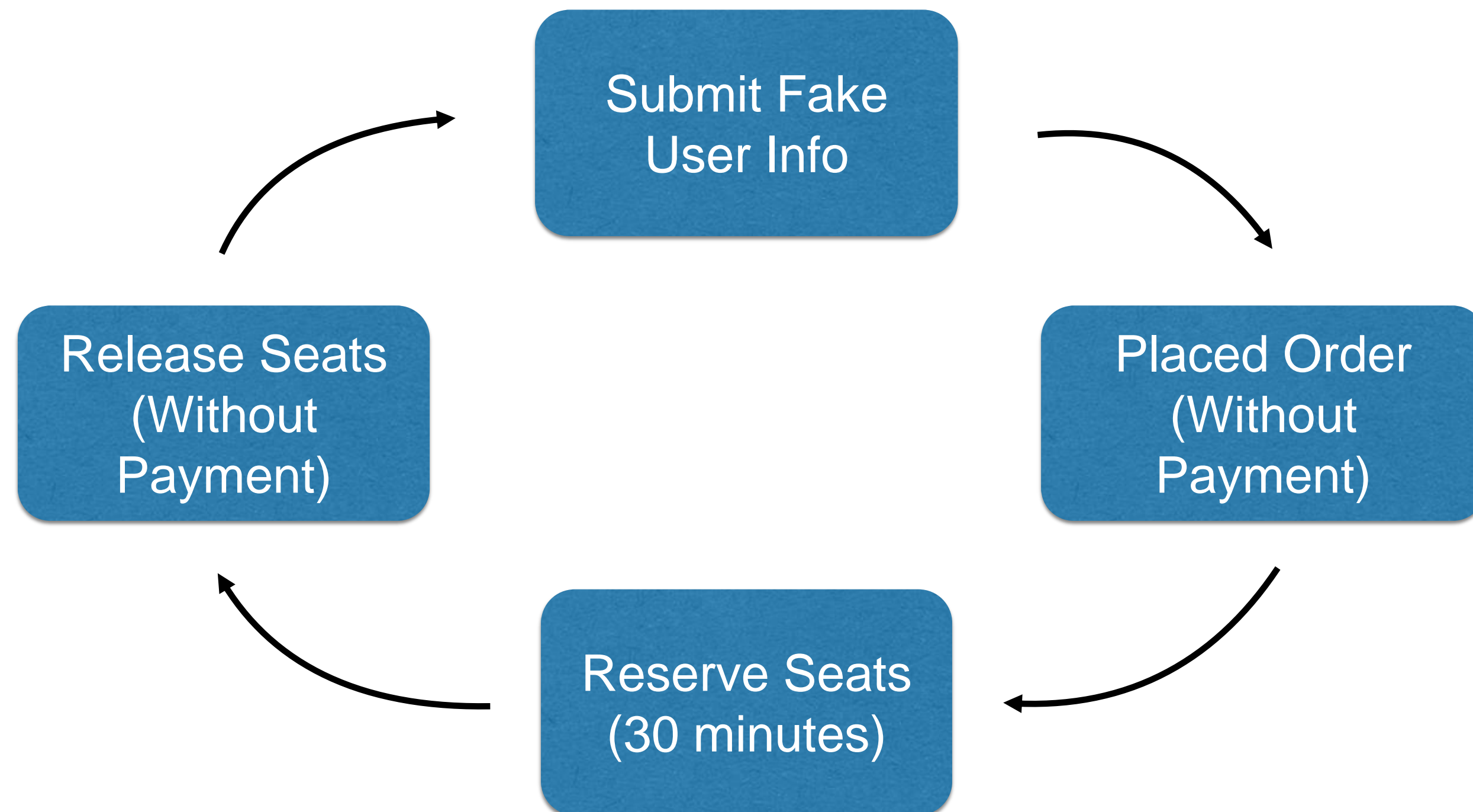High traffic volume but brings low income, as well as impact to customer experience

Lots of Malicious Traffic

- Fake User Info
- Taking more than 10s to load sites
- With un-explainable usage statistics

Million Dollar Revenue Loss

- Tickets always on-hold
- Low Attendance Rate
- Customer Loyalty Decrease

Hackers holding on to legitimate seats also put a lot of price pressure on AirAsia and its customers

Submit Fake User Info

Placed Order (Without Payment)

Reserve Seats (30 minutes)

Release Seats (Without Payment)

More Than Just Cloud

Alibaba Cloud
Official Cloud Services Partner

The Aviation Industry Anti Bot Attack Scenario

AirAsia Anti Bot Case Study: How to Anti Bot?

Alibaba Cloud employs the award-winning security products and the professional security services

Alibaba Cloud WAF Anti-Bot Protection

Client

IP Reputation

Bot Protection

Human-bot Identification

Expert Support

Server

e.g. Block the IDC or cloud IP, exception can be made by white list

Rate Analysis Based Blocking

Block the requests failed to pass Auth

Expert Support and Analysis
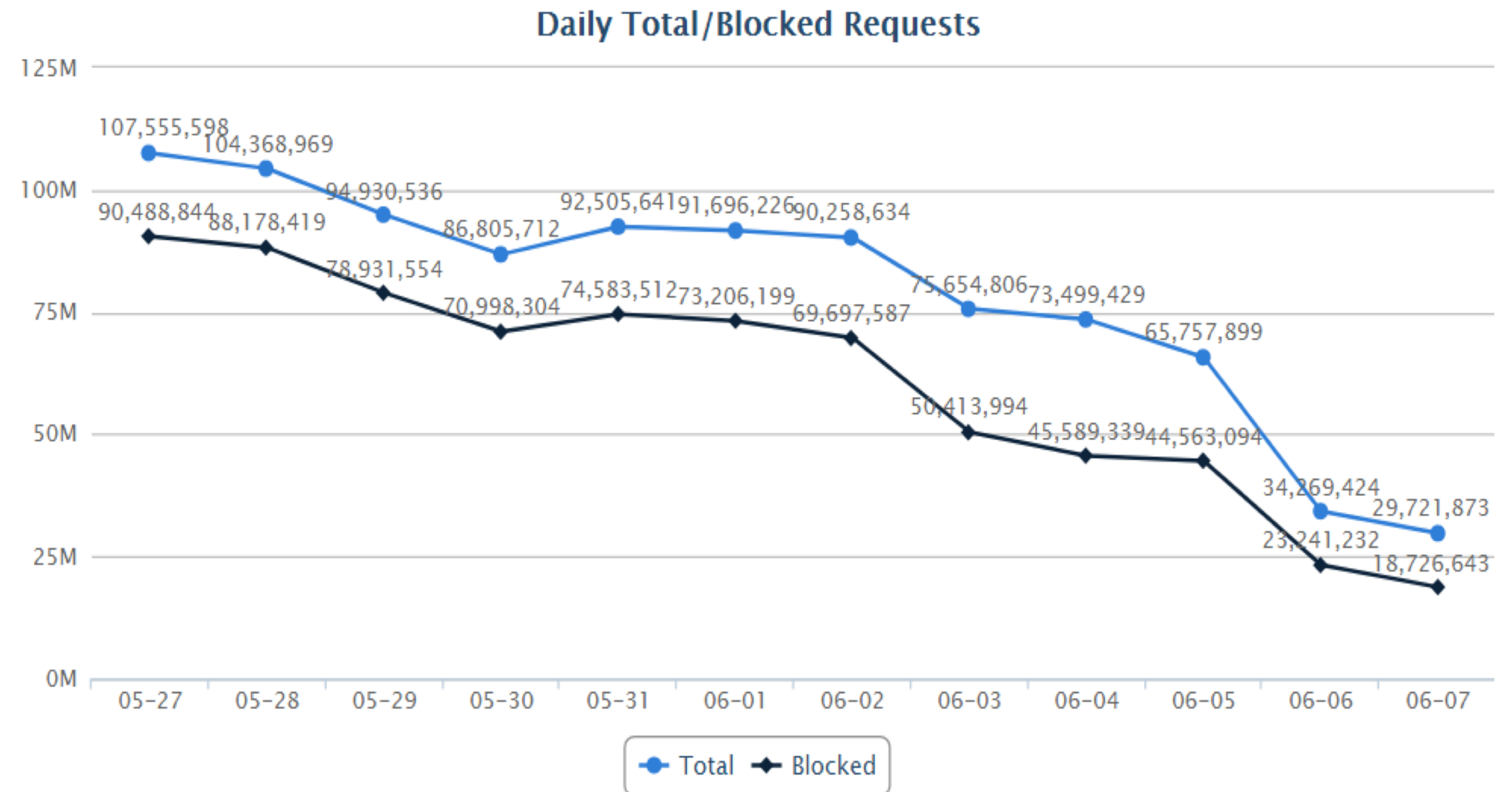
Legitimate Traffic

Bot Traffic
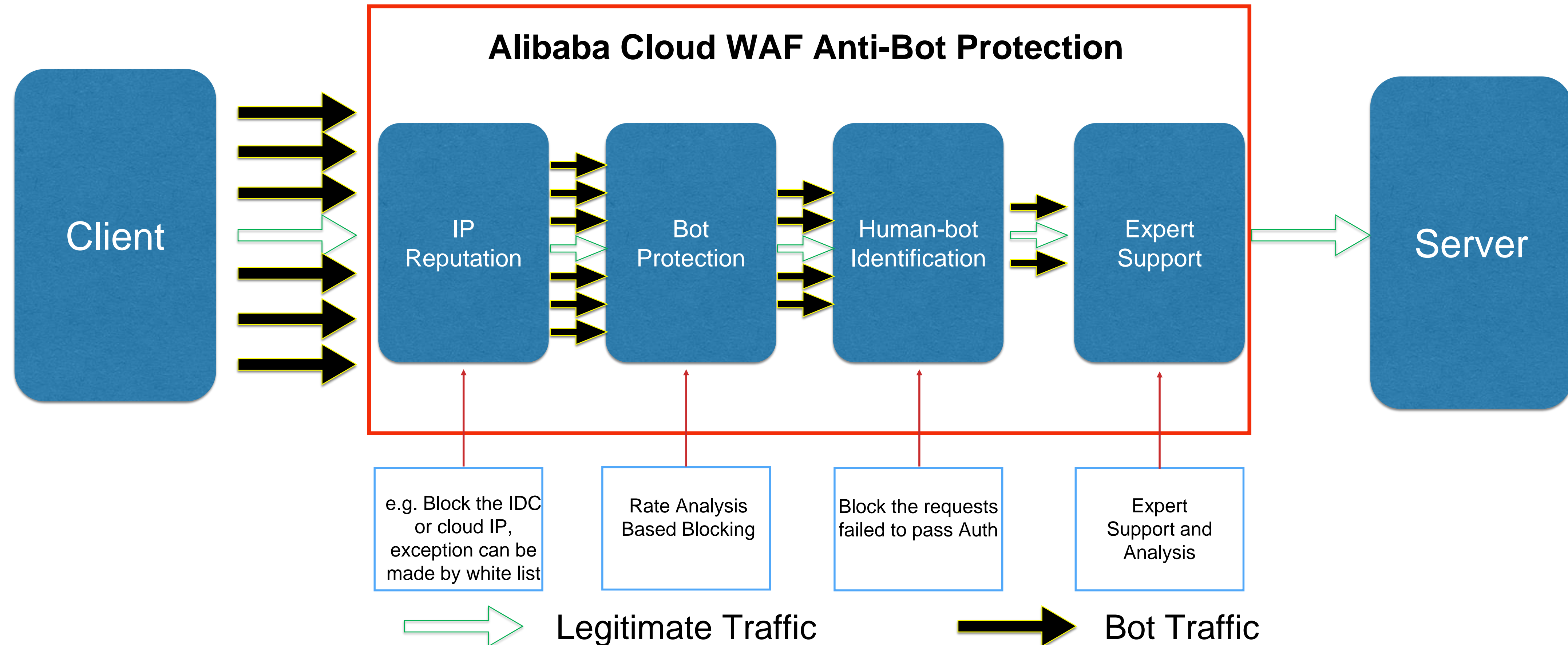
The Aviation Industry Anti Bot Attack Scenario

AirAsia Anti Bot Case Study: How About The Result?

The significant results achieved by the security solutions from Alibaba Cloud

- At the end of the **14 Day PoC** , average interception rate of bad traffic was **75%**
- PoC was successful with illegitimate traffic down by **72%**

- Employ the extensive CDN network on Alibaba Cloud in China
- Employ the award-winning security products from Alibaba Cloud
- Employ the professional security services from Alibaba Cloud

Daily Total/Blocked Requests

Total values:
107,555,598 · 104,368,969 · 94,930,536 · 86,805,712 · 92,505,641 · 91,696,226 · 90,258,634 · 75,654,806 · 73,499,429 · 65,757,899 · 34,369,424 · 29,721,873

Blocked values:
90,488,844 · 88,178,419 · 78,931,554 · 70,998,304 · 74,583,512 · 73,206,199 · 69,697,587 · 50,413,994 · 45,589,339 · 44,563,094 · 23,241,232 · 18,726,643

X-axis: 05-27, 05-28, 05-29, 05-30, 05-31, 06-01, 06-02, 06-03, 06-04, 06-05, 06-06, 06-07

Legend: Total — Blocked

More Than Just Cloud

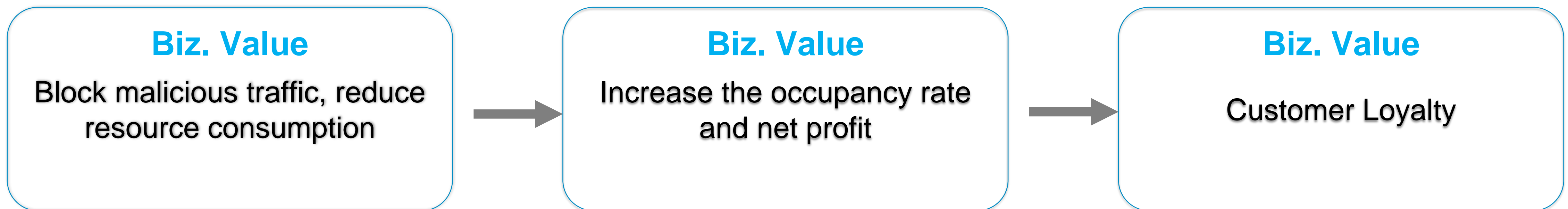# The Aviation Industry Anti Bot Attack Scenario

AirAsia Anti Bot Case Study: Decision To Alibaba Cloud!

AirAsia decided to move all the protection of its source systems to Alibaba Cloud

"We need Alibaba Cloud continue to give us the support and assistance in fixing our issues."
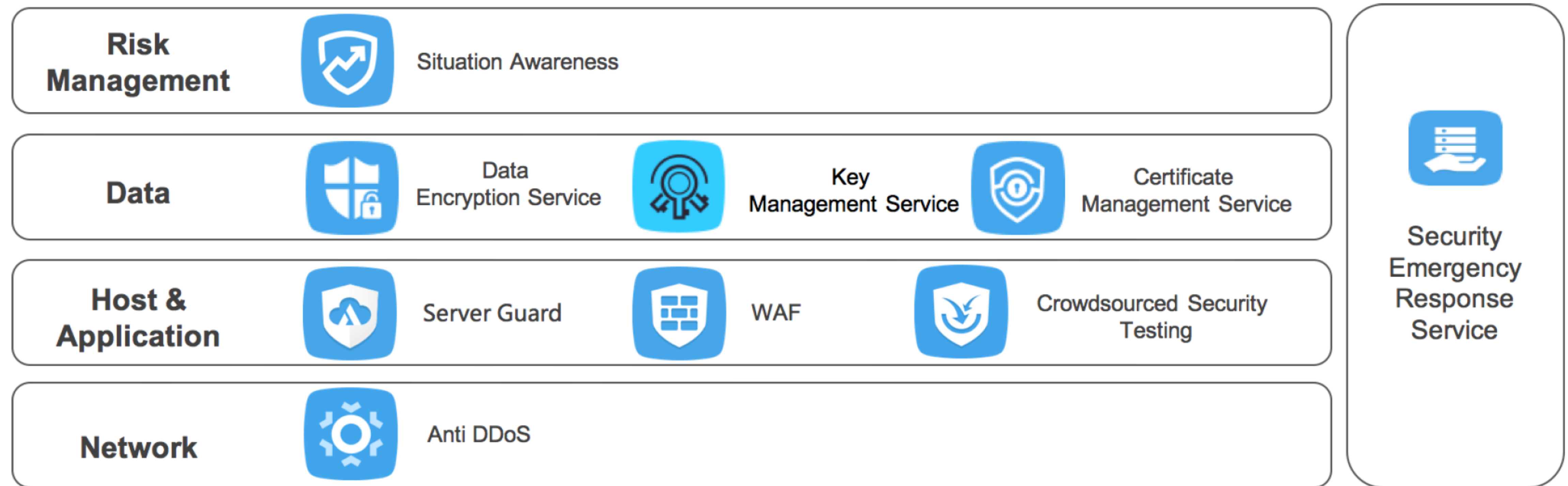
Declan –AirAsia Group CIO.

Biz. Value	**Biz. Value**	**Biz. Value**
Block malicious traffic, reduce resource consumption	Increase the occupancy rate and net profit	Customer Loyalty

Alibaba Cloud Security Service Family

Anti Bot is one important function of WAF product. Alibaba Cloud can provide all-around Security Protection for you

Risk Management	Situation Awareness			
Data	Data Encryption Service	Key Management Service	Certificate Management Service	
Host & Application	Server Guard	WAF	Crowdsourced Security Testing	
Network	Anti DDoS			

Security Emergency Response Service

Alibaba Cloud | MORE THAN JUST CLOUD