



# Genie Solution Introduction

GenieATM & GenieAnalytics

Genie Networks

September 2020



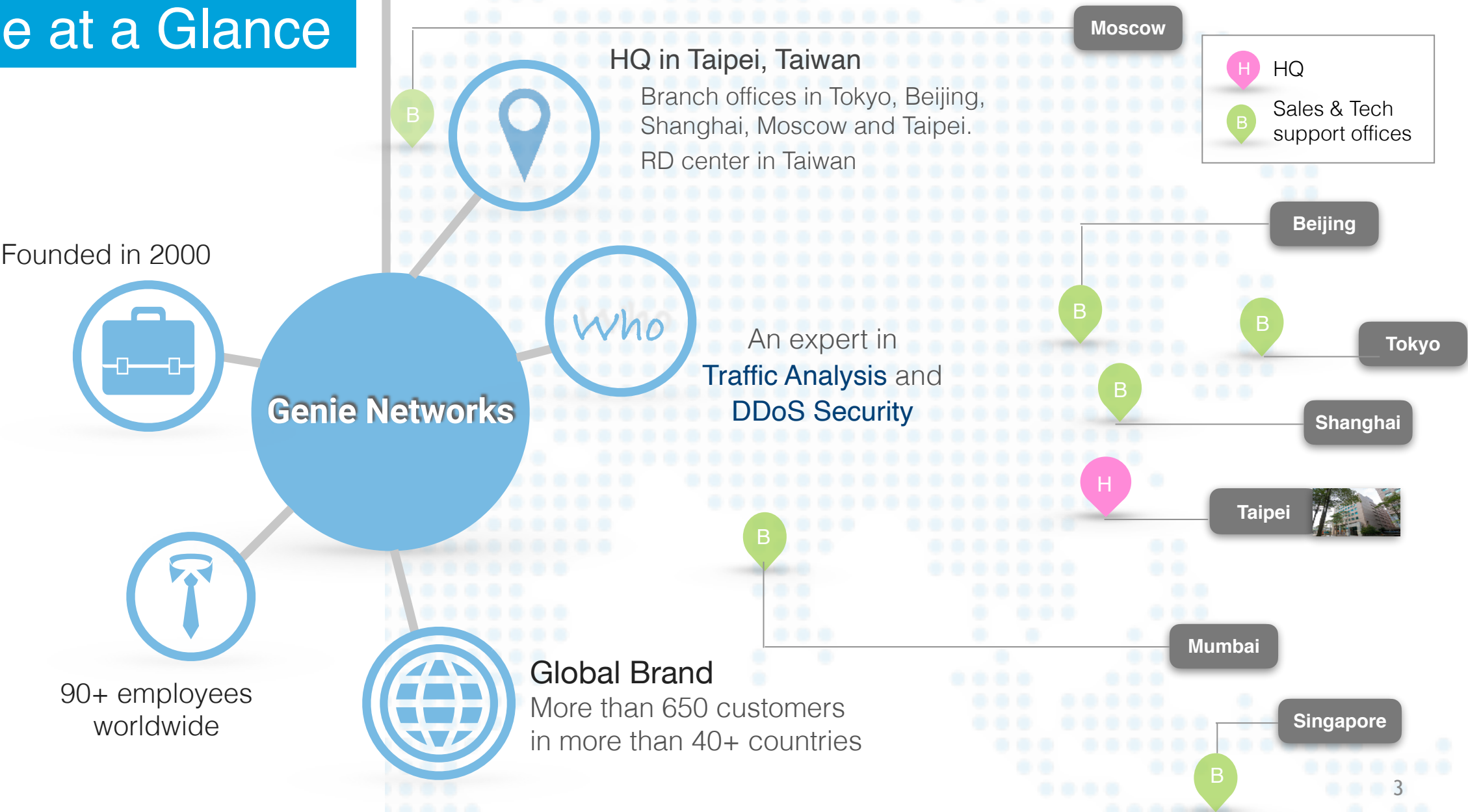
# Agenda

---

- About Genie
- Why Genie Solution?
- What is Genie Solution?
  - GenieATM
  - GenieAnalytics
- Success Stories
- Summary of Benefits



# Genie at a Glance



# Why Genie Solution?

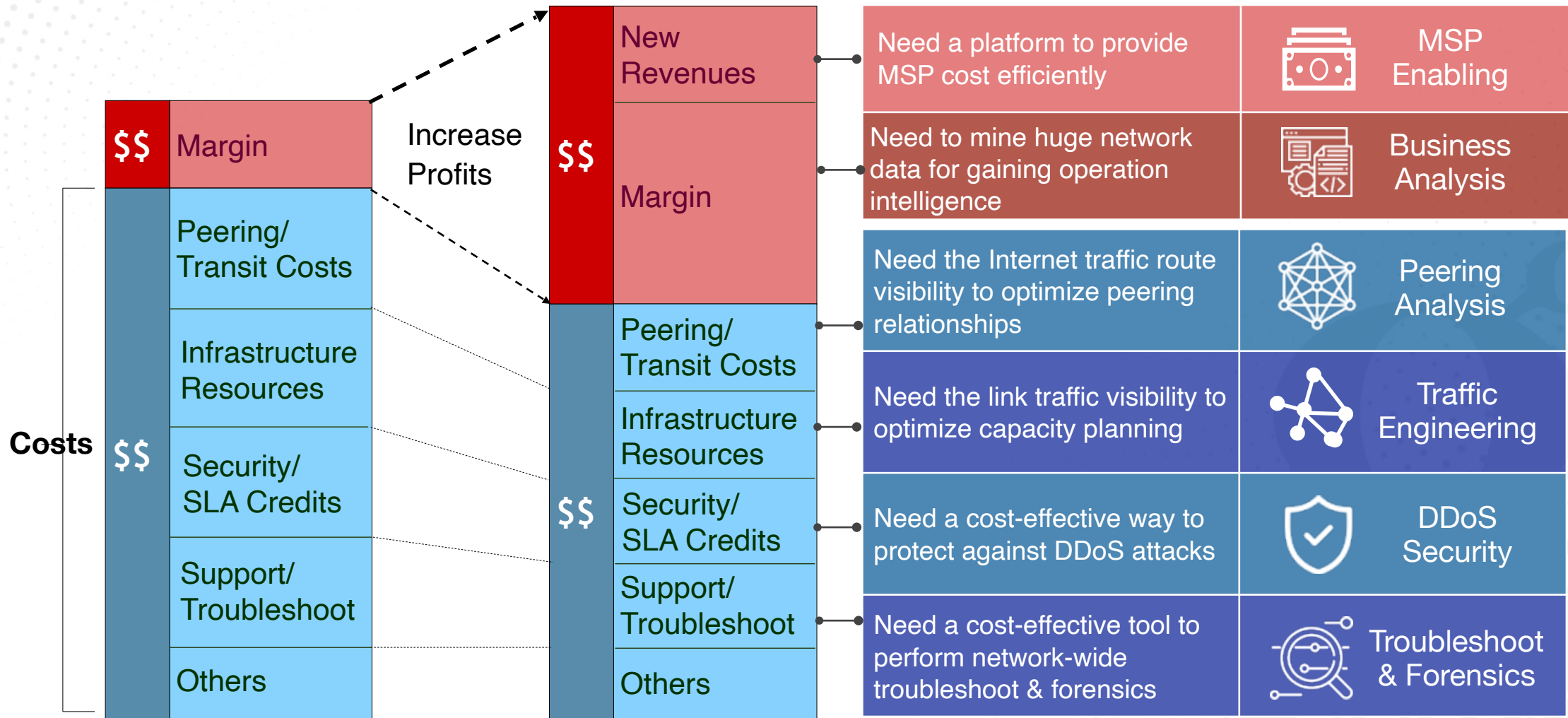
---





# Service Provider Challenges & Needs

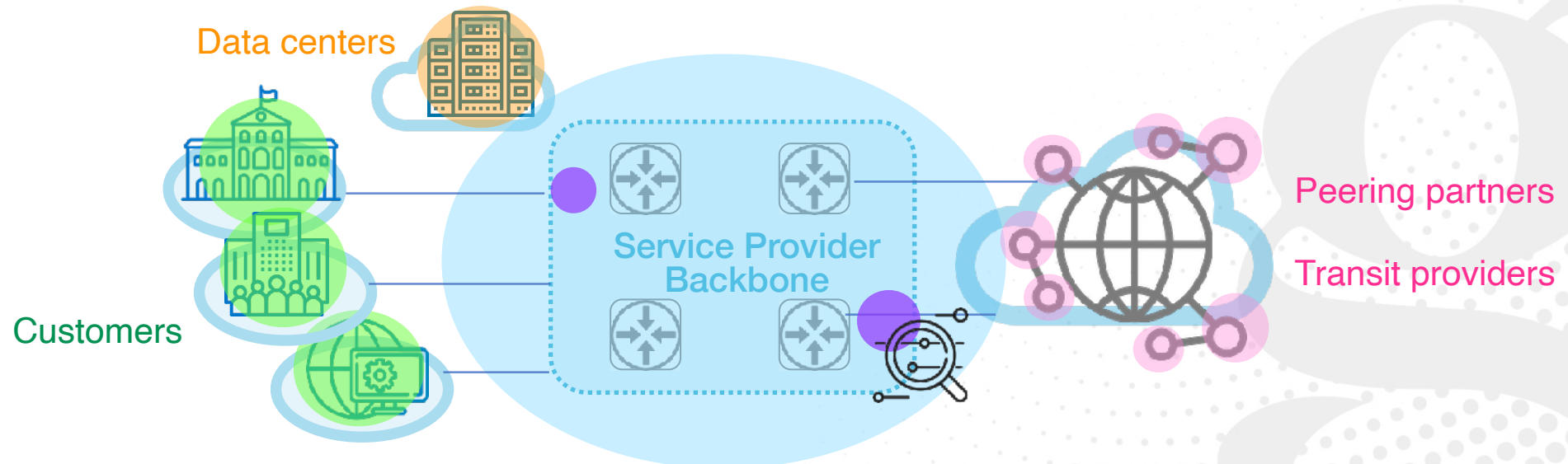
Reducing operation/security costs, and increasing revenues.



# The Need | Visibility is King

## Need network-wide, end-to-end synthetic traffic visibility to answer operation questions

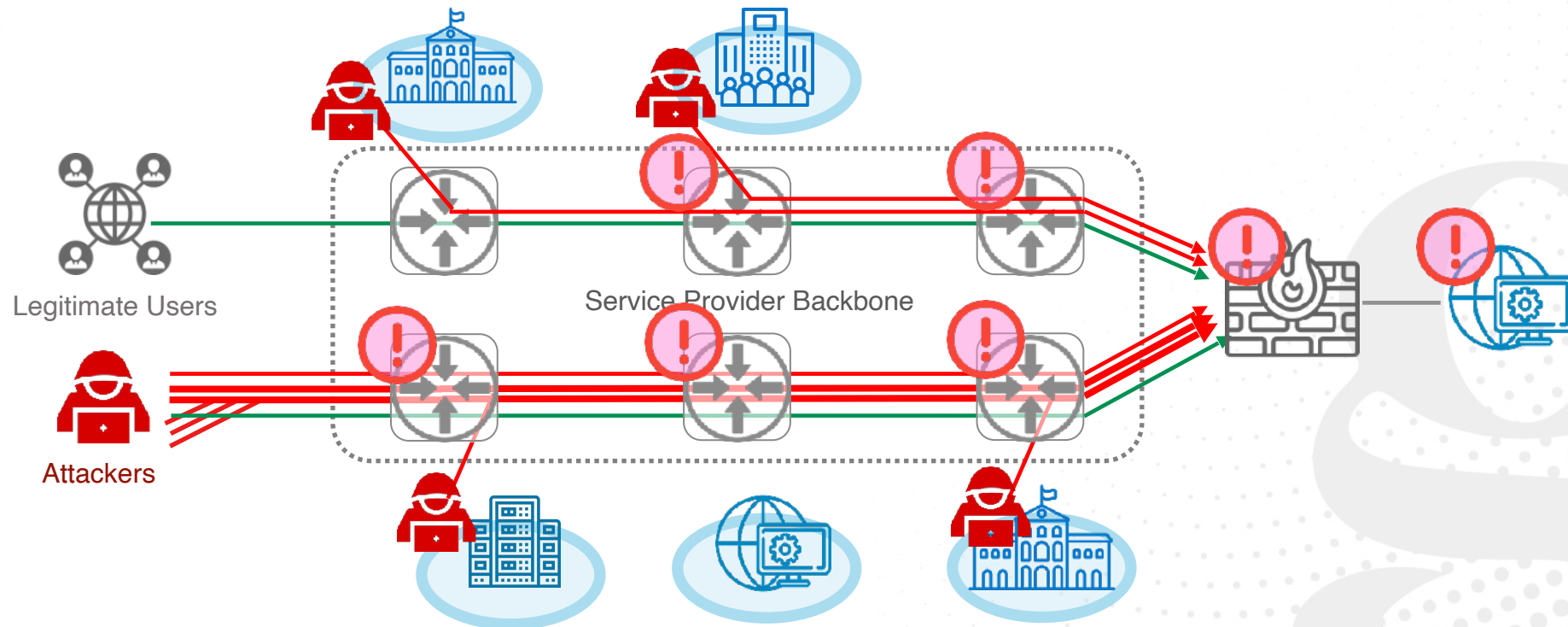
- Data sources from multiple network devices (routers, switches, DNS servers, etc.) everywhere in the networks
- Correlated intelligence of traffic flows, SNMP data, BGP routes, DNS queries, RADIUS, etc.
- Network model intelligence for aggregating data correctly



# The Need | Complete DDoS Defense for SPs

## Need a cost-effective network-wide DDoS defense

Distributed attacks come from anywhere of the network. Each individual source's traffic may appear normal, yet collectively the network is still harmed and DoSed. It paralyzes not only the target victims, but also the network infrastructure. **Last-mile, in-line DDoS protection is not enough!**



# What is Genie Solution?

---





# Value Propositions

## Traffic Analysis



Network  
Planning



Traffic  
Engineering



Peering  
Analysis



Trouble-  
shooting



Business  
Analysis



**GenieATM**



**GenieAnalytics**



Infrastructure  
Security



Cloud-based  
DDoS Security



Network  
Forensics

## DDoS Security

GenieATM

---



# Scalable Architecture

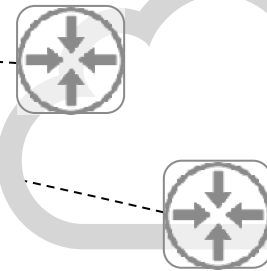
Carrier-grade Capacity

## Centralized Architecture

■ genie

### GenieATM Controller

For a small deployment, one standalone Controller to do all the tasks, from data collection, reporting to detection.



## Distributed Architecture

■ genie

### GenieATM Controller

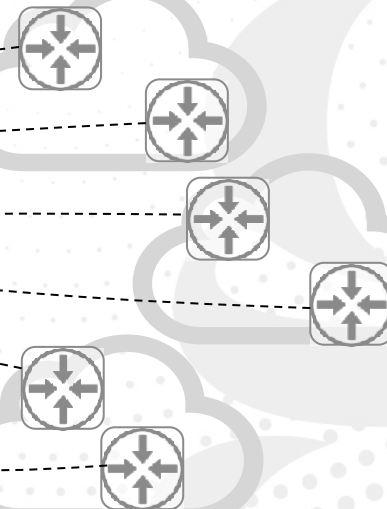
■ genie

■ genie

■ genie

### GenieATM Collectors

For larger deployments, adding more Collectors to scale up the solution scale.



# GenieATM Core Functionality

Network-wide Visibility & DDoS Security

## 01 Collect Network Info

Including BGP messages, SNMP MIBs, and Flow-based telemetry

## 02 Analyze & Visualization

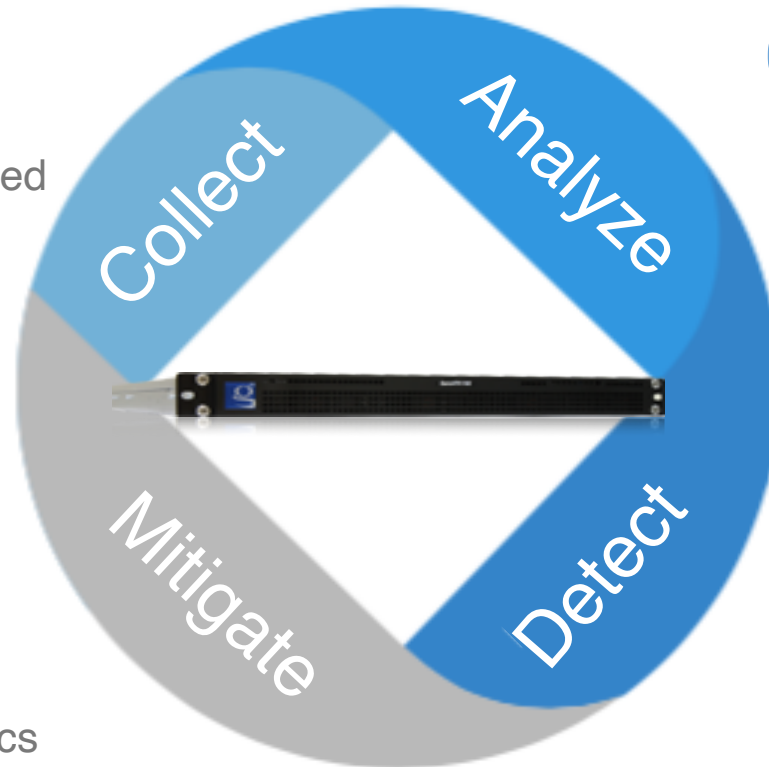
Real-time and historical network-wide traffic reports

## 04 Act on Anomalies

Alert and mitigate detected events and incident forensics

## 03 Detect Anomalies

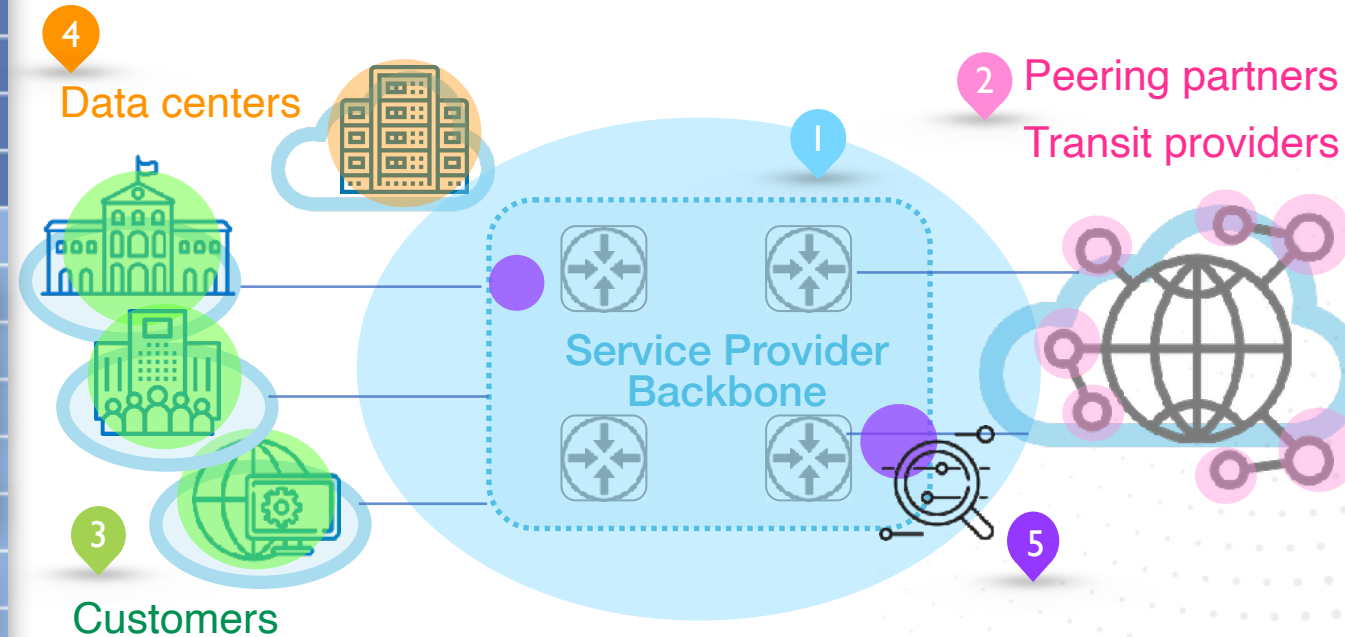
Detect DDoS, worms, zero-day attacks and BGP route instability



# Operation Intelligence-based Visibility

## Network-wide monitoring on user customizable network objects

- Abundant analysis reports for various network objects (e.g., Internet, Peer/Transit neighbors, Customer sub-networks, Server farms, etc.)
- Embedded network topology to avoid over-counting issues



Drilldown

Trend

Top-N

Breakdown

Matrix





# Comprehensive DDoS Defense



## Collect

Pervasive traffic data  
collected from  
multiple routers/  
switches



## Detect

Behavior analysis-  
based detection with  
learned baselines and  
fast alerting



## Mitigate

Various action options  
including blackholing,  
FlowSpec, and Out-Of-  
Path (OOP) cleaning

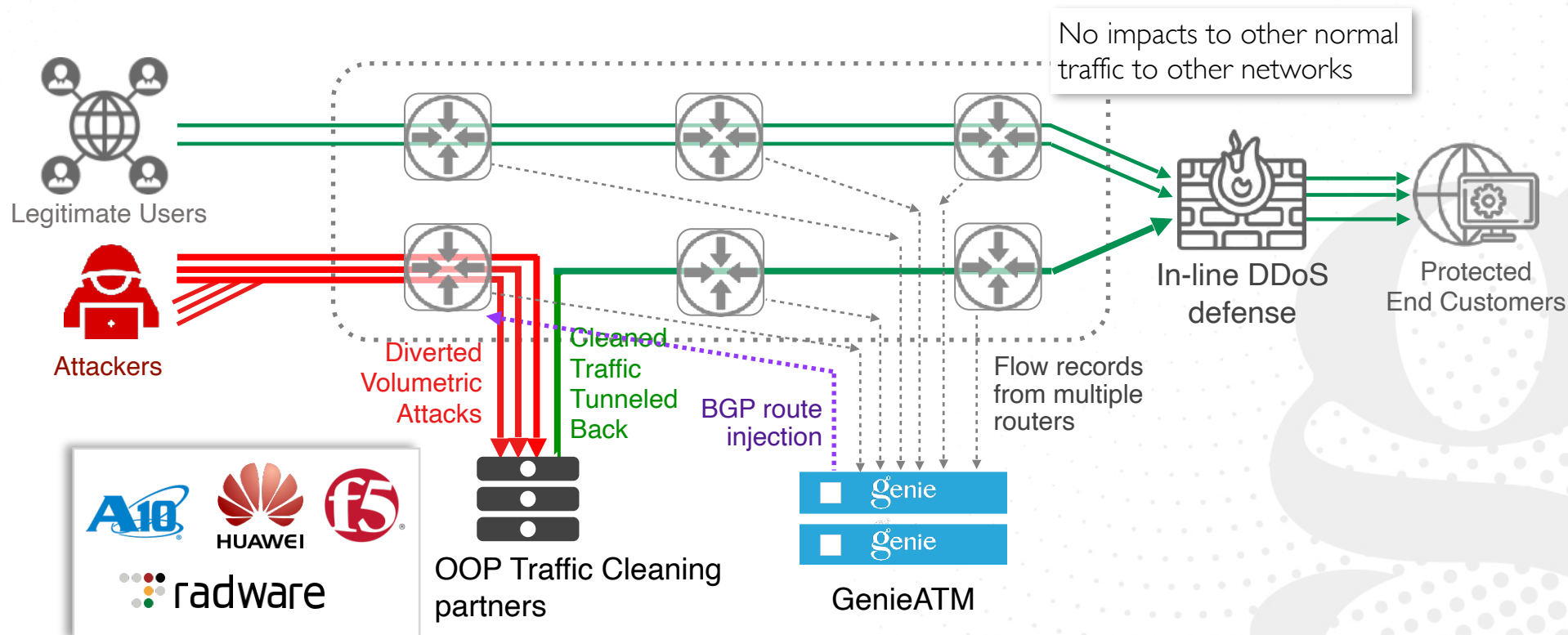


## Forensics

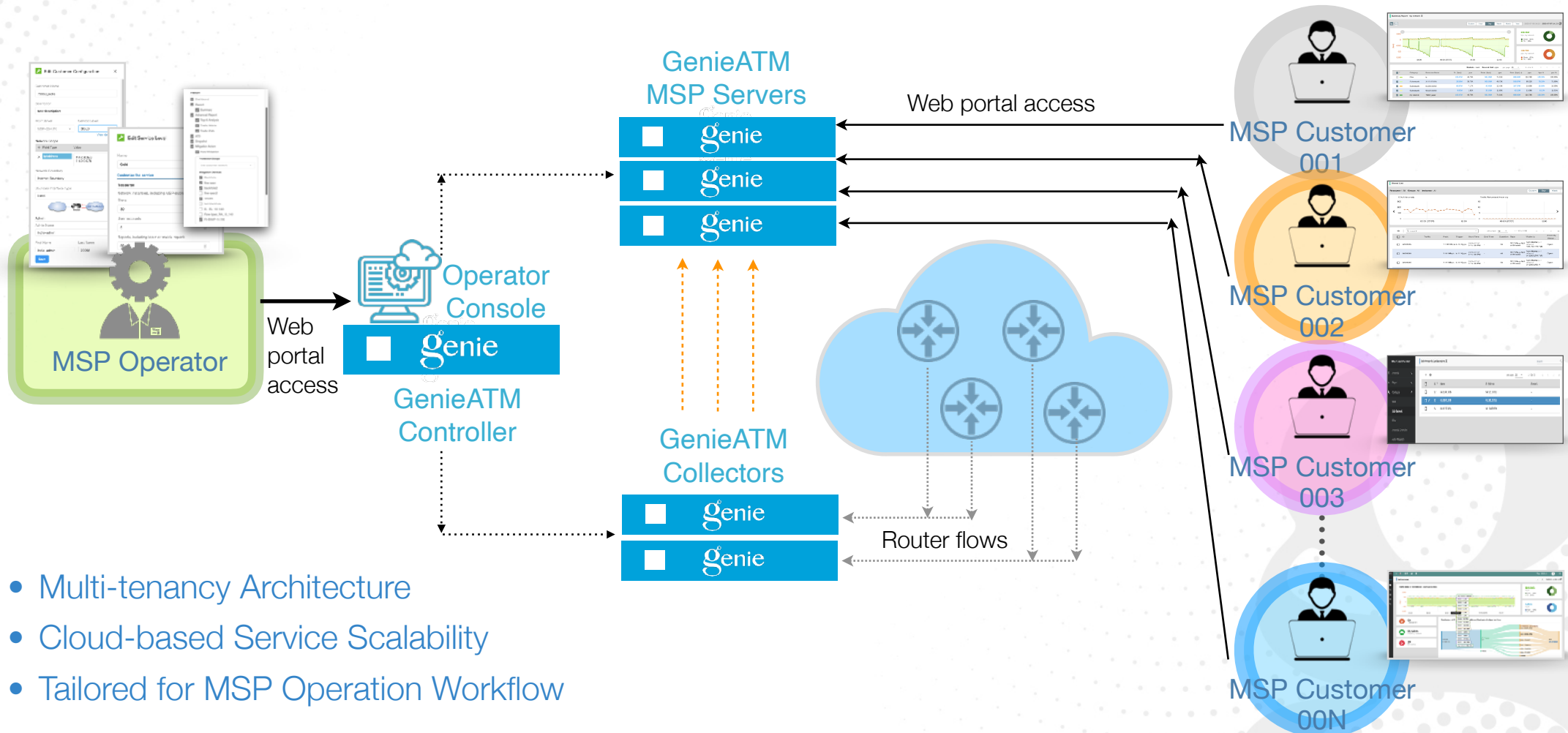
Instant troubleshooting  
tool & direct linkage to  
GenieAnalytics for attack  
forensics

# OOP with Traffic Cleaning Partners

- ◎ **DISTRIBUTED DATA COLLECTION:** pervasive traffic data from the entire infrastructure
- ◎ **CENTRALIZED INTELLIGENCE:** network-wide, cross-segmental analysis for detection
- ◎ **LOW DEPLOYMENT COST:** flow-based detection & shared OOP cleaning centers
- ◎ **BEST OF BREED:** integrate with 3rd party detectors for detection and cleaning



# MSP Enabling



# GenieATM Highlights



## FAST DETECTION

Automatic  
learning to  
detect DDoS  
within seconds



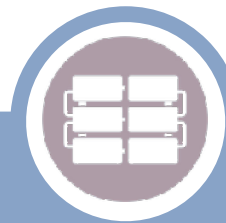
## FLEXIBLE REPORTS

Customizable  
reports with fast  
report response  
time



## SCALABLE ARCHITECTURE

Stackable  
capacity with its  
distributed  
architecture



## HIGH AVAILABILITY

Redundancy  
from collection,  
analysis to  
deporting



## COST EFFECTIVE

Network-wide  
solution by  
utilizing Flows &  
OOP defense

GenieAnalytics

---





# GenieAnalytics: A Big Data Extension to GenieATM

## 01 Big Data Capability

Ad-hoc analytics without pre-configuration on stored data (w/o aggregation or pre-filtered)



## 02 Fast Raw Data Process

Compression and sampling mechanisms to handle long term data storage

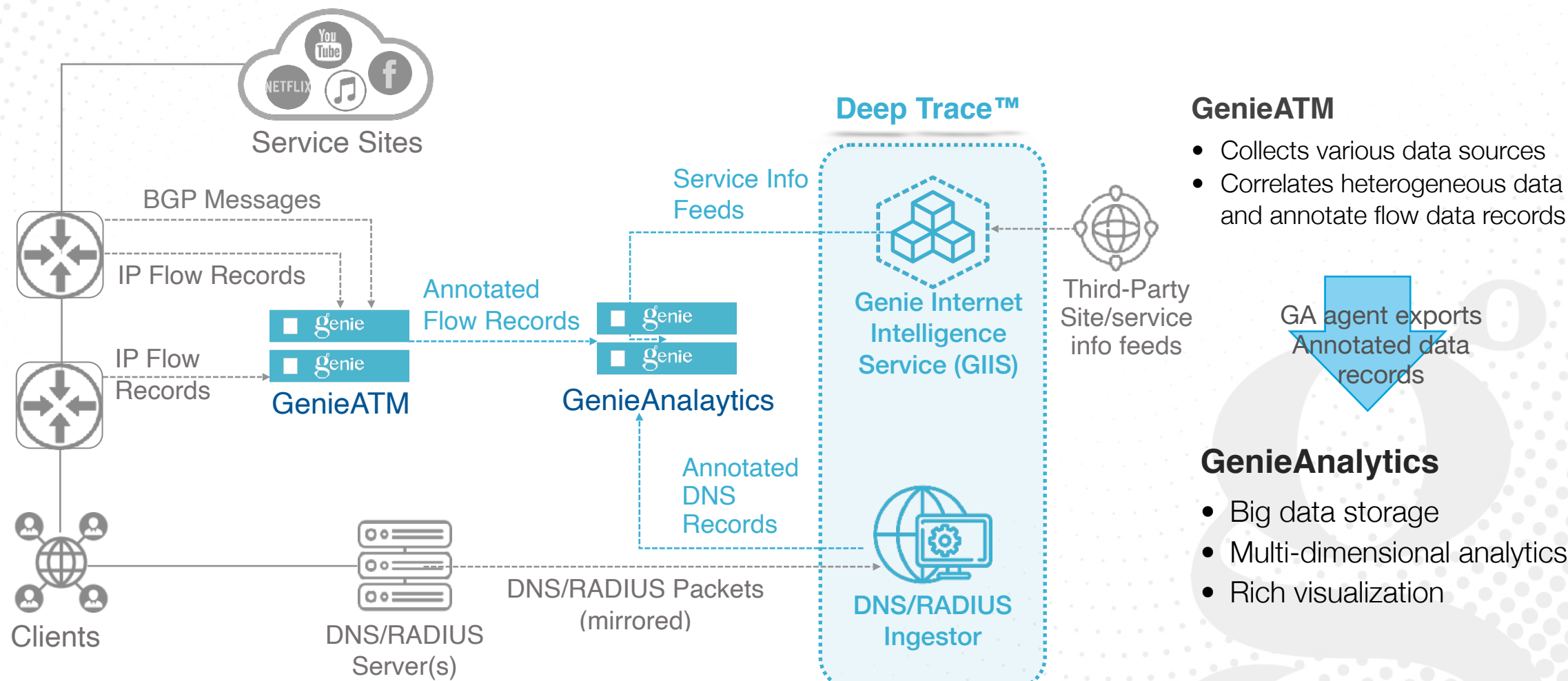
## 04 More Data Correlation

Fusing more heterogeneous data for richer analytic context (incl. geo-location, DNS, RADIUS, proprietary DB)

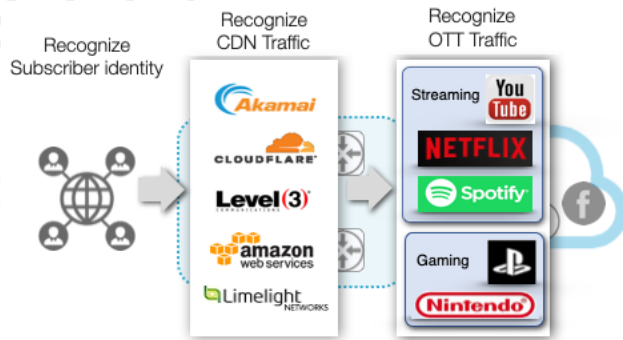
## 03 Powerful Visualization

Responsive UI, various charts, and multifaceted dashboards

# GenieAnalytics Deployment

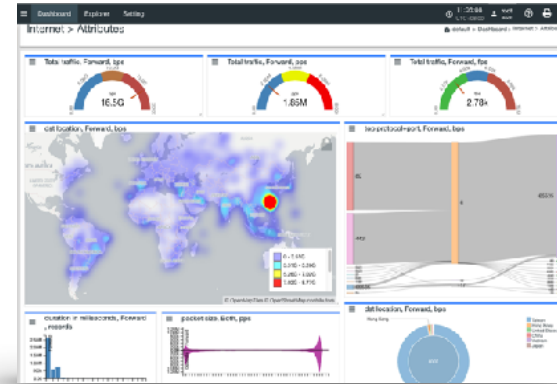


# Powerful Big Data Analytics & Rich Visualization



## Multi-dimensional Pipeline

Interactive big data exploration with unlimited Filter combination and analytic aggregation keys.



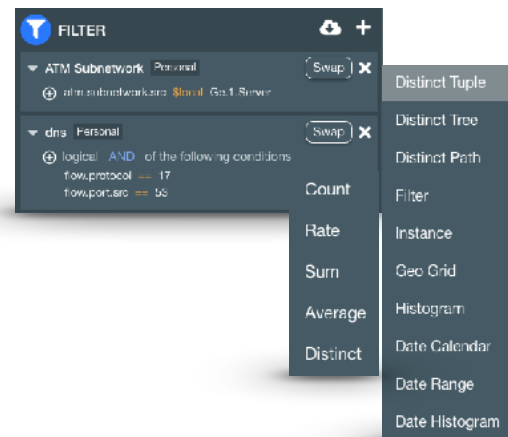
## Multi-tenant Architecture

A Customer user can see only analyze his own network's traffic and can build his own dashboard.



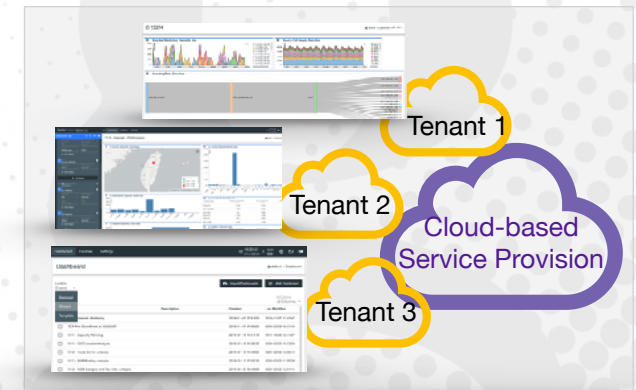
## Enriched data

Provide rich analytic context (e.g., OTT service, CDN, subscriber identity) by fusing heterogeneous data (incl. geo-location, DNS, RADIUS, and proprietary DB.)



## User-friendly Dashboard

A Customer user can define his own dashboard with various analytic pipelines, charts and layout with live-update.



# GenieAnalytics Highlights



## COMPRESSED STORAGE

Resampling and compression to support years-long data storage



## ADVANCED DASHBOARD

Unified view across various analytic perspectives, incl. widgets & time spans



## GRANULAR ANALYTICS

Multi-dimension, ad-hoc analytics as granular as 1 second



## RICH ANALYTIC CONTEXT

Correlation & intelligence for analyzing by OTT, CDN, subscriber



## COST EFFECTIVE

Economic solution for equivalent Big Data capability and capacity

# Case Studies

---





# Reduce CAPEX/OPEX at the eService Company



A digital services company that engages in gaming, eSports, eCommerce and digital finance, primarily focusing on Southeast Asia and has local presences in different regional markets.

## Business Drivers

- Rising traffic volumes requiring better capacity planning for CAPEX reduction
- Requiring traffic insights efficiently for OPEX reduction

## Genie Solution

- 1 x GenieATM as a Flow data collector and DDoS detection
- 1 x GenieAnalytics as a traffic analytics tool

## Business Challenges

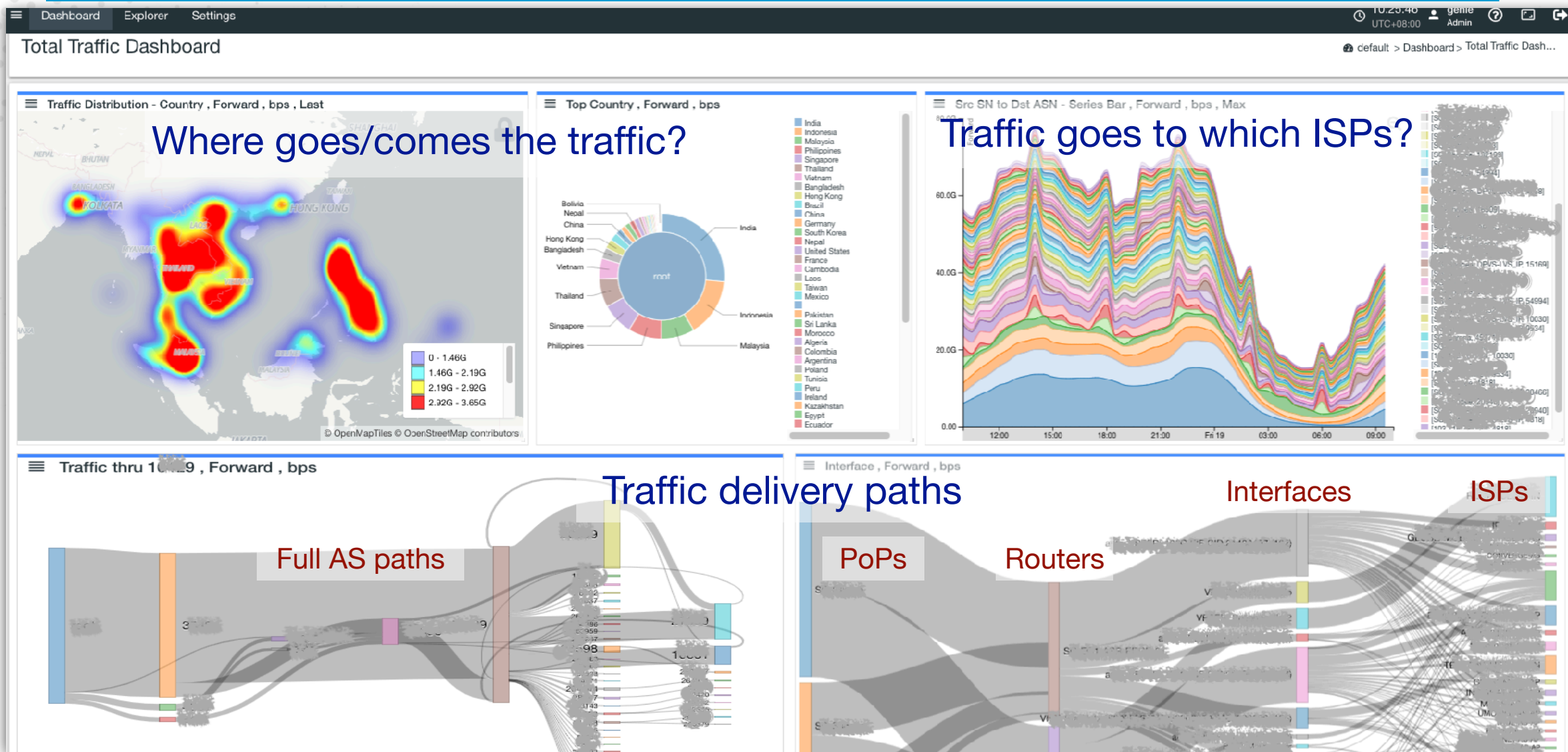
- Big traffic data volume
- Complex network requires flexible multi-dimensional analytic capability
- Various analytics demands require intuitive visualization

## Why Genie

- Efficient computation and storage resource requirement
- Fast & flexible big data analytics
- Powerful analytic dashboard & charts

## Rich Analytic Visualization

## Capacity Planning & Optimization



# Increase Revenues by Managed Security Services

S

A tier-1 telecommunications company, which provides wireline and mobile telecommunications services, including voice, Internet, data centers and other related information and application services.

## Business Drivers

- DDoS have grown in sizes and frequency, making it challenging to protect network infrastructures
- Delivering in-cloud, managed DDoS defense services to increase revenues

## Genie Solution

- 10 x GenieATM as a Flow data collector and DDoS detection
- 2 GenieATM MSP Servers as MSSP enablers
- Traffic cleaning devices

## Business Challenges

- Defend network-wide DDoS to protect its infrastructure
- A platform to easily enable managed services
- Carrier-grade performance, performance and reliability

## Why Genie

- A ready cost-effective, multi-tenant platform
- MSP business aligned workflow design
- Carrier-grade system scalability and high availability

# Enabling MSSP Services

## DDoS Security

**Anomaly Detection Configuration**

Severe event : over 3 minutes | Recovery latency : 3 minutes

ID	Name	bps Threshold	Unit	pps Threshold	Status
1	TCP SYN Flooding	20.00	Kpps	2.00	Enabled
2	IP Protocol Null	2.00	Kpps	2.00	Enabled
3	TCP Flag Null or Misuse	5.00	Kpps	5.00	Enabled
4	Malform TCP with port 0	10.00	Kpps	10.00	Enabled
5	Malform UDP with port 0	-	Disabled	-	Disabled

**Mitigation**

Protection IP Address: 183.192.199.142/32

Action Type: Rate Limit by Flow-Spec

Traffic Rate Limit: Rate: 3, Unit: Gbps

Additional Parameters:

Source IP Address: Source IP

Type: HTTP Flooding

Protocol: TCP(S), UDP(L), ICMP(I)

Port: Port

Destination: Destination Port

Source: Source Port

Save

**Event List**

Time Window 3 day(s) 2020-01-16 00:00

Granularity: 1 Hour

Filter(1) : Event Active Time : 2020-01-15 18:00:00

ID	Traffic	Sev
149024	566	566
149023	2.2	2.2

**Event Detail 149023 - 2020-01-15 18:26:00**

117.136.8.231 my network  
Recovered TCP SYN Flooding  
58800364% > 11 bps

Start	Peak	End	Average
2020-01-15 18:28:00	18:28:00	-	-
2.20 Mbps	-	-	-

**Drill-down Top-n Analysis**

Source Origin ASN	Origin ASN (Local)	bps	pps
CMNET-V4SHANGHAI-AS-AP Shanghai Mobile Communications Co. Ltd (24400)	426.69M	56.07K	

Source IP Country	ipCountryId (Local)	bps	pps
CHINA(17230)	479.38M	64.46K	

Multi-tenant detection  
& mitigation for each  
MSSP customer

# Enabling MSSP Services

## Traffic Visibility

Multi-tenant portal of  
scoped traffic visibility  
for MSSP customers

description

MSP Customer 002

Network Alias

Service Level

Service Level: **SILVER**

Maximum Number of Network Instances: : 10

Maximum Number of User Accounts: 10

Maximum Number of Reports: 10

Mitigation Service: **On**

Auto-Mitigation: **On**

Protection Scope: 5Registered IP addresses

[more...](#)

Network Scope

IP prefix or IP range

59.120.0.0/16

61.230.0.0/16

31.13.87.0/24

Mitigation Device

Flowspec-msp customer

Blackhole-msp customer

Feature

☐ Dashboard

☒ Report

☒ Summary

☐ Advanced Report

☐ Top-N Analysis

☐ Traffic Matrix

☐ Traffic Path

☒ ATD

☐ Snapshot

☒ Mitigation Action

☒ Auto-Mitigation

Protection Scope

registered IPs, with

Number of protected IP addresses

5

Mitigation Devices

☐ F5

☐ PRTG

Summary Report - my network

Custom

1 Hour

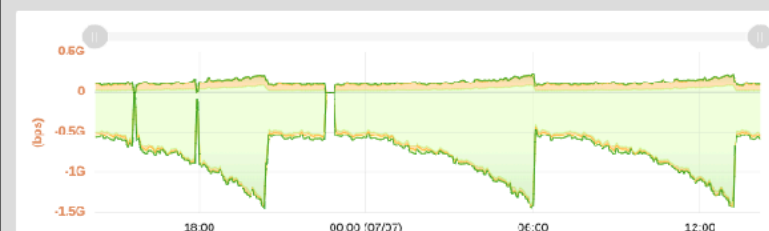
Day

Week

Month

Year

2020-07-06 14:13 - 2020-07-07 14:13



688.46M

bps, my network

From : 85%

To : 15%

118.79K

pps, my network

From : 62%

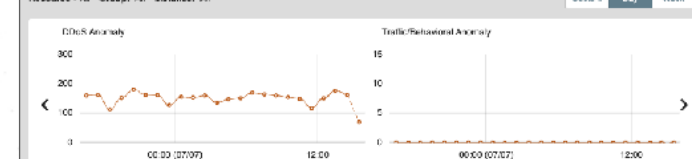
To : 38%

Statistic : Last Second Unit : pps per page: 25 1 - 4 of 4

	Category	Resource Name	To (bps)	pps	From (bps)	pps	Sum (bps)	pps	bps %	pps %
<input type="checkbox"/>	Filter	h	106.47M	44.78K	581.38M	74.01K	688.46M	118.79K	100.00%	100.00%
<input checked="" type="checkbox"/>	Subnetwork	31.13.87.0/24	29.58M	35.79K	509.39M	49.73K	538.97M	85.52K	78.29%	71.99%
<input checked="" type="checkbox"/>	Subnetwork	61.230.0.0/16	66.97M	7.17K	40.40M	12.43K	107.37M	19.60K	15.50%	16.50%
<input checked="" type="checkbox"/>	Subnetwork	59.120.0.0/16	9.93M	1.82K	32.19M	11.85K	42.12M	13.68K	6.12%	11.51%
<input checked="" type="checkbox"/>	my network	70067_japan	106.47M	44.78K	581.38M	74.01K	688.46M	118.79K	100.00%	100.00%

Event List

Resource : All Group: All Instance: All



ID	Traffic	Peak	Trigger	Start Time	End Time	Duration	Type	Victim IP	Attack Status
<input type="checkbox"/> A0038	1.18 Mbps	5.72 Kpps	2020-07-07 01:10:30	-	58	2020-07-07 01:10:30	TCP Flood (SYN or RST)	Non Home (11.152.144.138)	Open
<input type="checkbox"/> A0038	2.42 Mbps	5.77 Kpps	2020-07-07 01:10:30	-	58	2020-07-07 01:10:30	TCP Flood (SYN or RST)	Non Home (11.152.144.138)	Open

# Summary of Benefits

---





# Value Propositions



## Holistic Visibility

Cost efficient by collecting & correlating Flows, BGP, SNMP, DNS and RADIUS



## In-depth Analytics

Model-based fast analytics and context-rich ad-hoc analytics



## Fast Detection

Automatic behavior-based detection within seconds



## MSP Enabling

Business-aligned, multi-tenant solution with scalability



## Carrier-grade Solution

Market-leading capacity, performance, scalability and High Availability (HA)

# THANK YOU!

• [www.genie-networks.com](http://www.genie-networks.com)

