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

Founded in 2000

90+ employees worldwide

Genie Networks

HQ in Taipei, Taiwan

Branch offices in Tokyo, Beijing, Shanghai, Moscow and Taipei.

RD center in Taiwan

An expert in **Traffic Analysis** and **DDoS Security**

Global Brand

More than 650 customers in more than 40+ countries

- Moscow
- Beijing
- Tokyo
- Shanghai
- Taipei 
- Mumbai
- Singapore

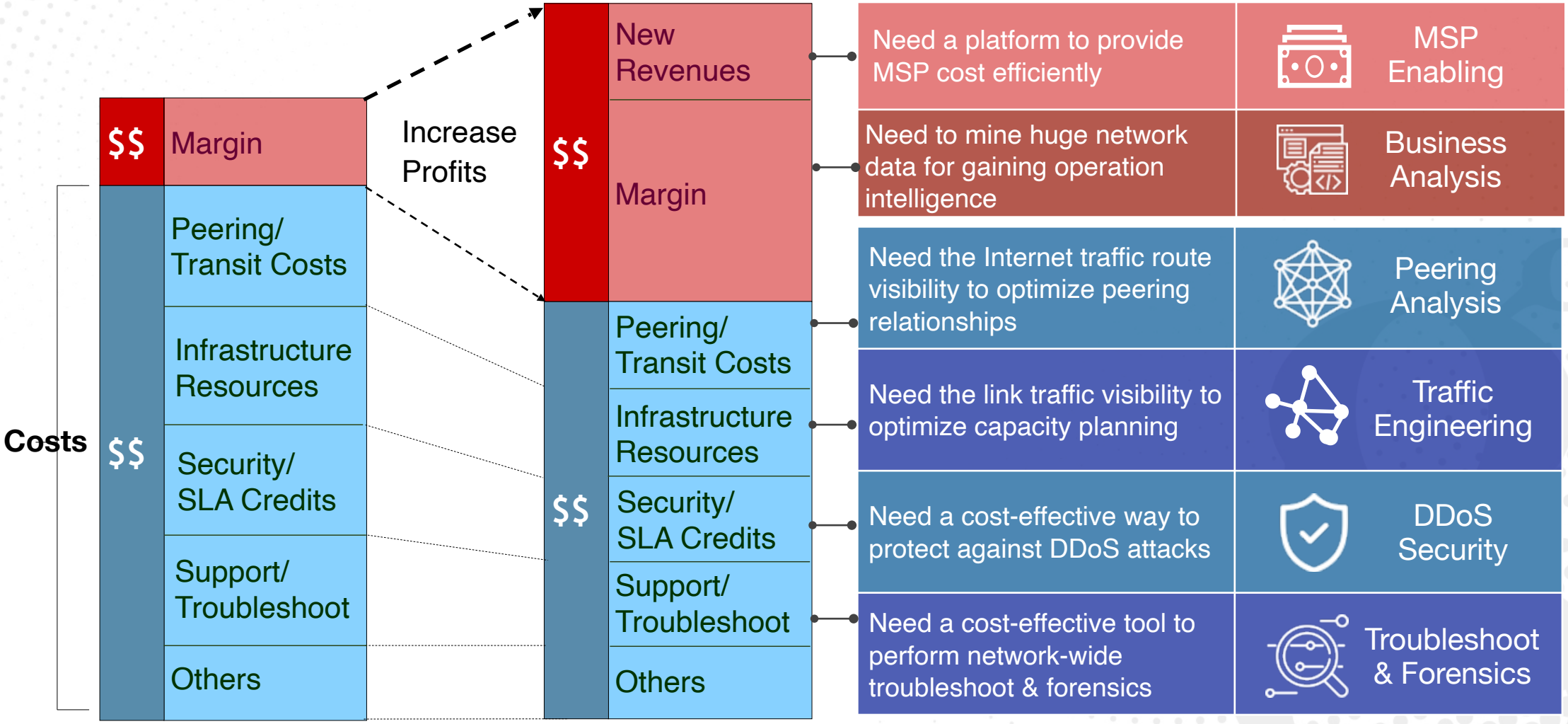
H HQ

B Sales & Tech support offices

Why Genie Solution?

Service Provider Challenges & Needs

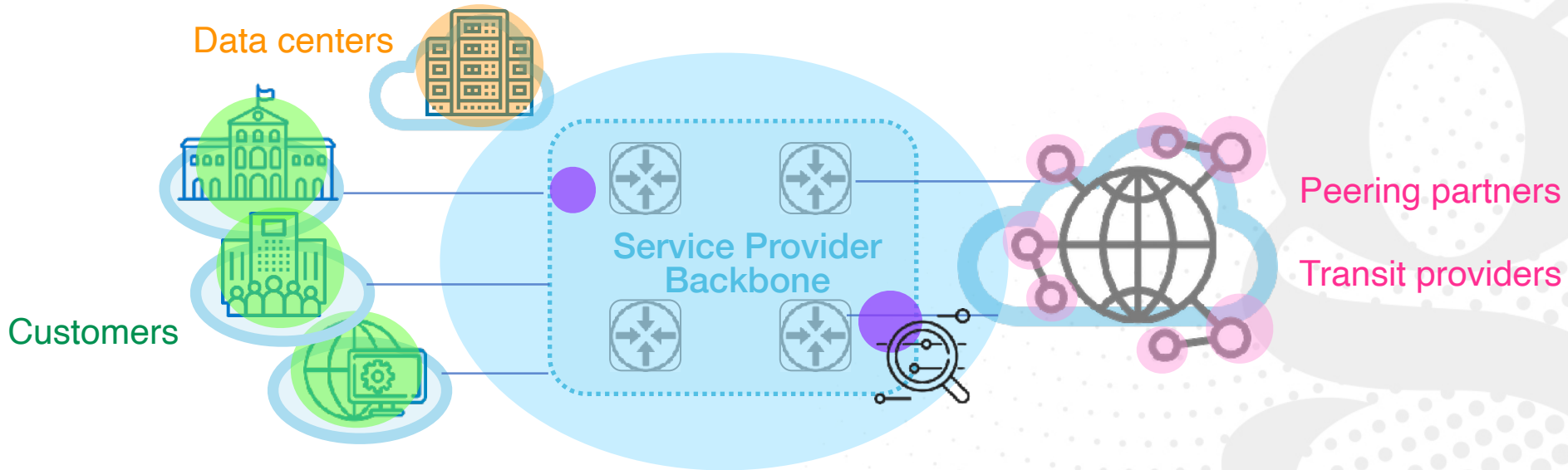
Reducing operation/security costs, and increasing revenues.



The Need | Visibility is King

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

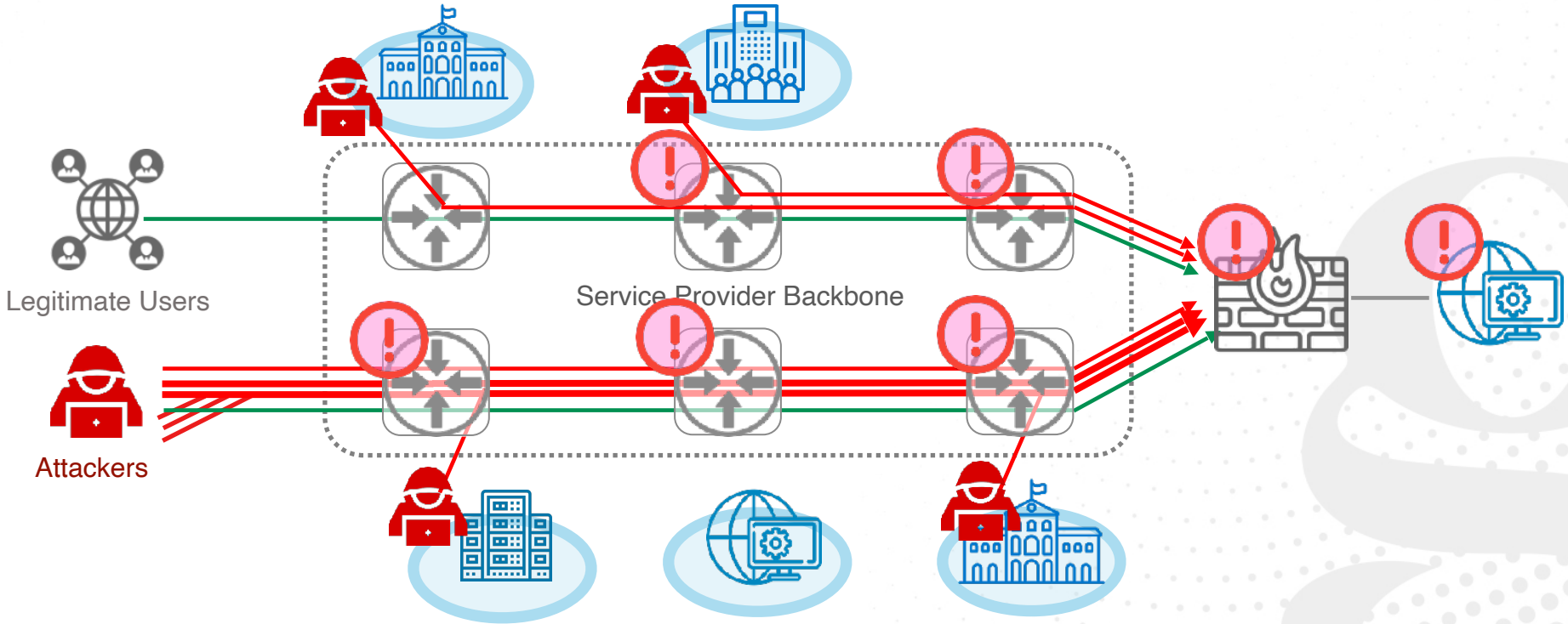
- Data sources from multiple network devices (routers, switches, DNS servers, etc.) everywhere in the networks
- Correlated intelligence of traffic flows, SNMP data, BGP routes, DNS queries, RADIUS, etc.
- Network model intelligence for aggregating data correctly



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?

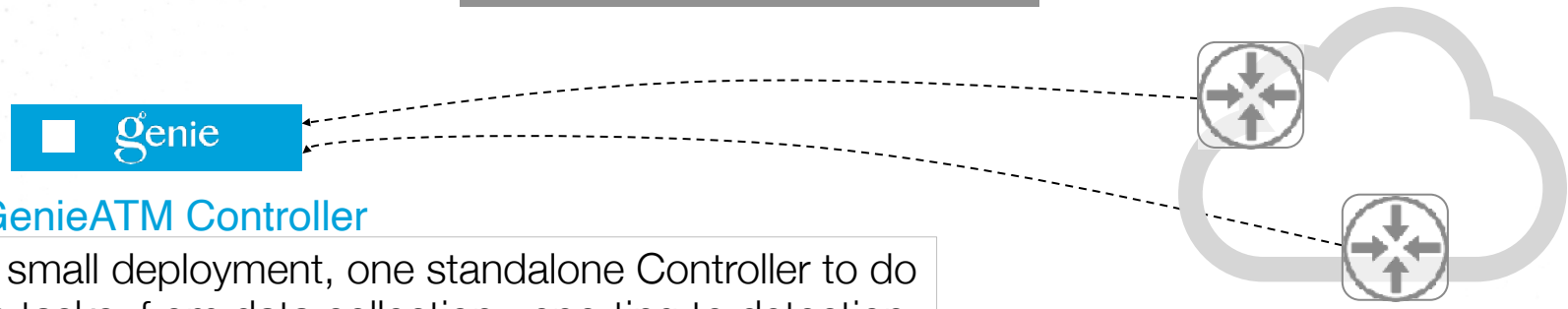
Value Propositions

GenieATM

Scalable Architecture

Carrier-grade Capacity

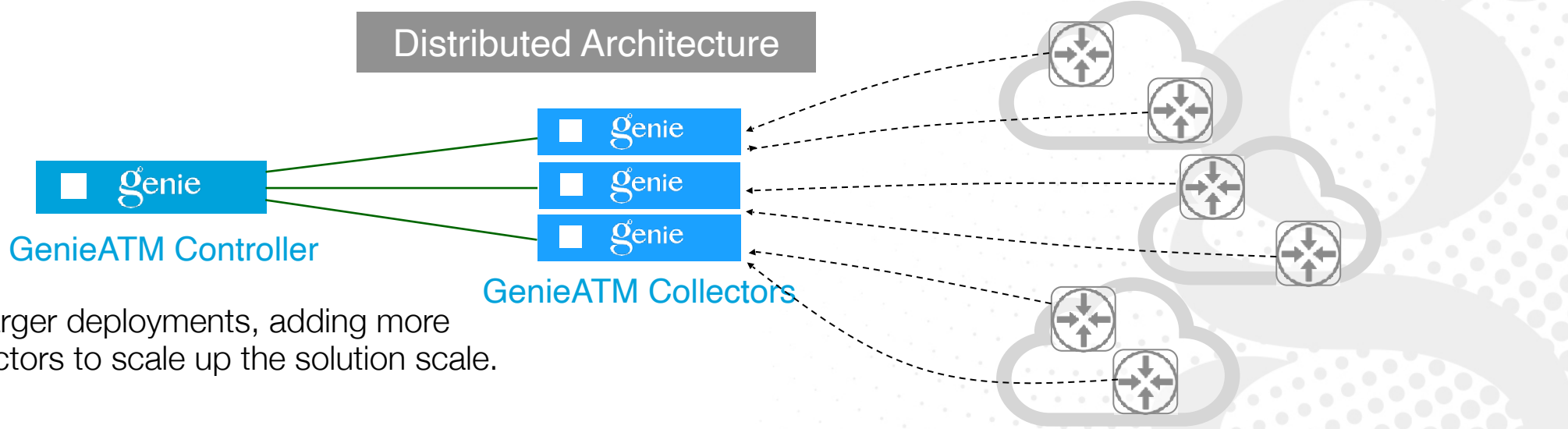
Centralized Architecture



GenieATM Controller

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

Distributed Architecture



GenieATM Controller

GenieATM Collectors

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

GenieATM Core Functionality

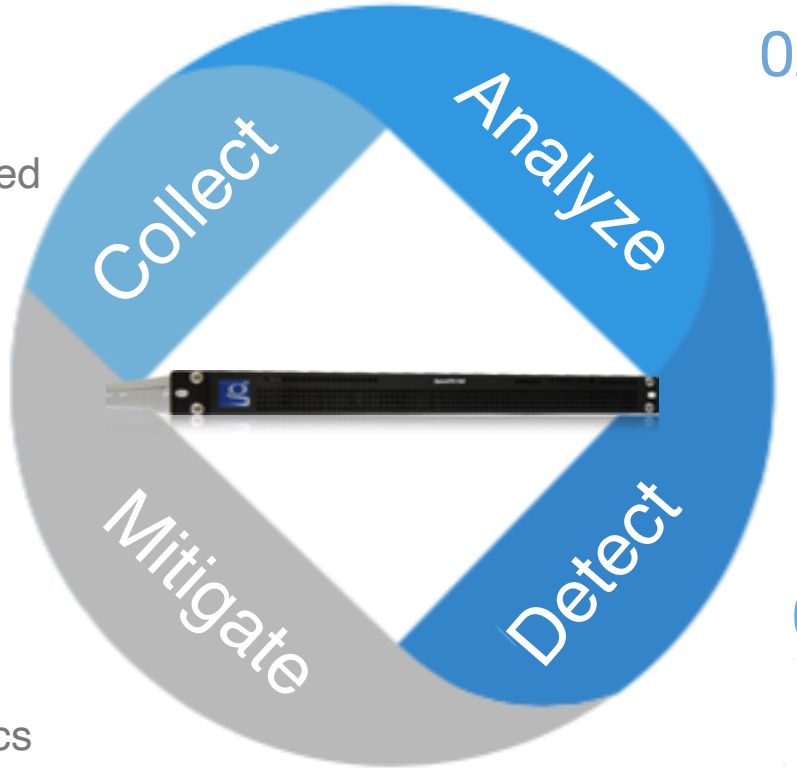
Network-wide Visibility & DDoS Security

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

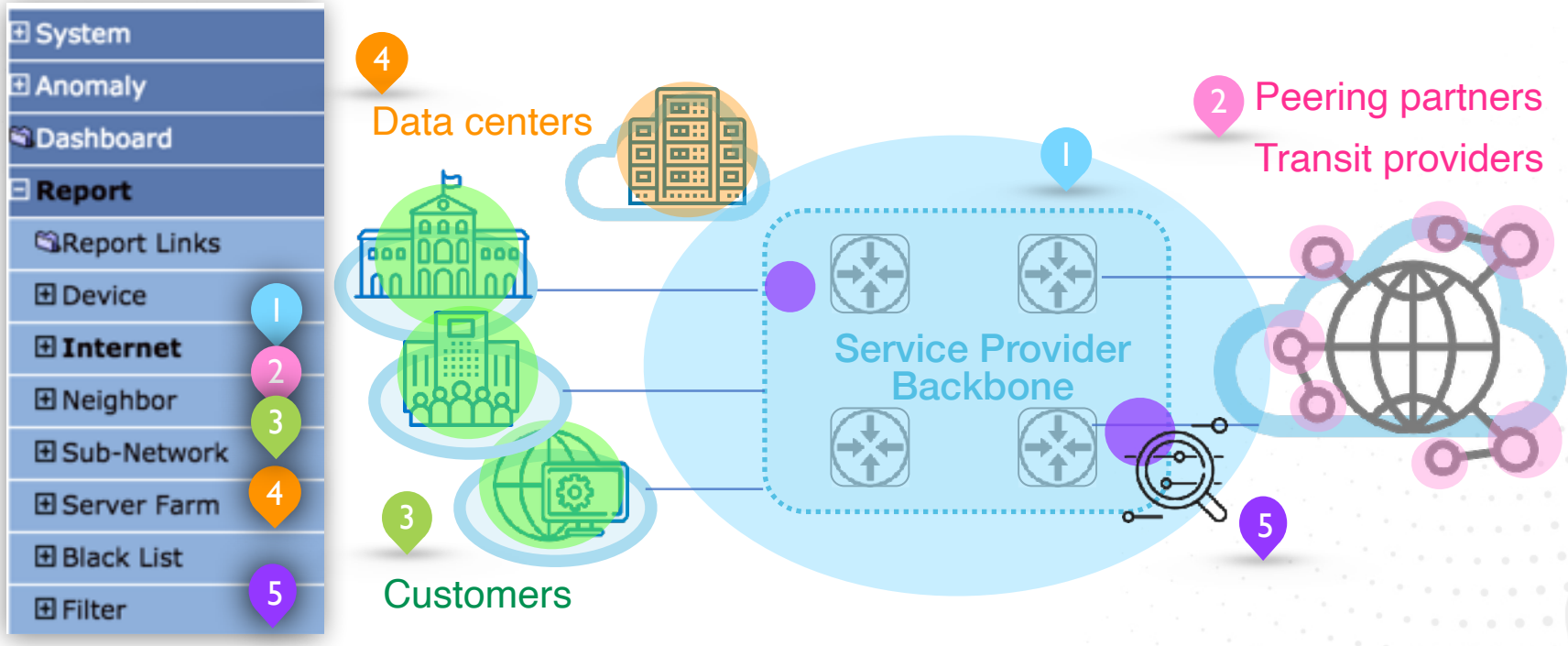
03 Detect Anomalies

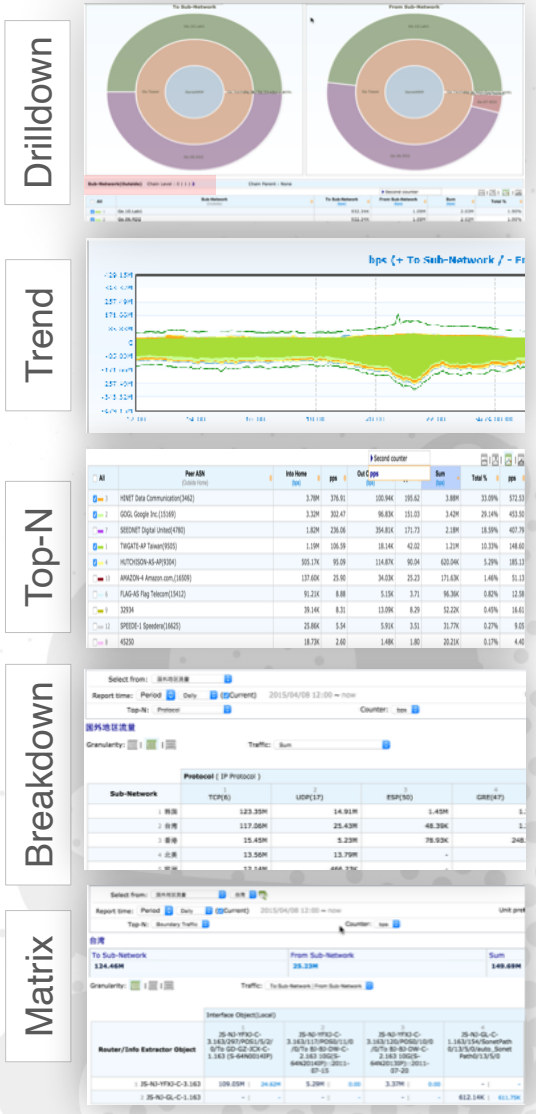
Detect DDoS, worms, zero-day attacks and BGP route instability

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





Comprehensive DDoS Defense

Collect

Pervasive traffic data collected from multiple routers/ switches

Detect

Behavior analysis-based detection with learned baselines and fast alerting

Mitigate

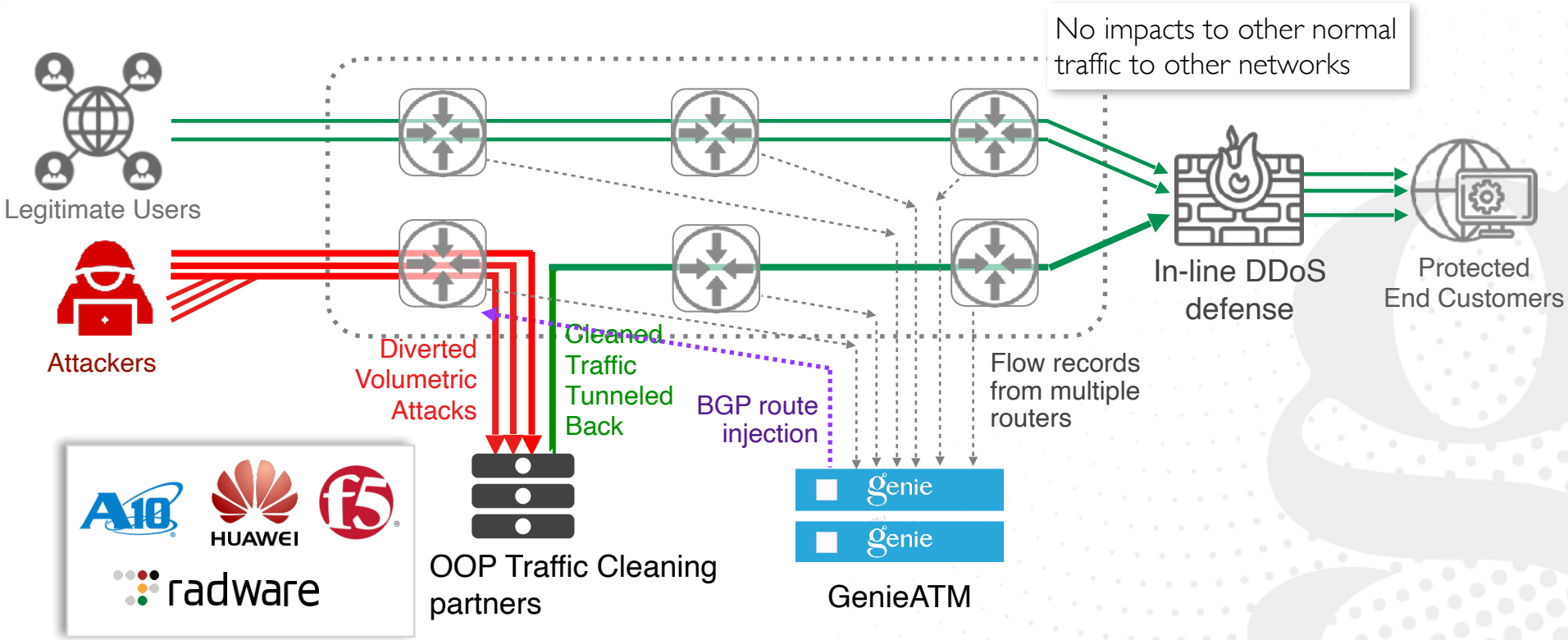
Various action options including blackholing, FlowSpec, and Out-Of-Path (OOP) cleaning

Forensics

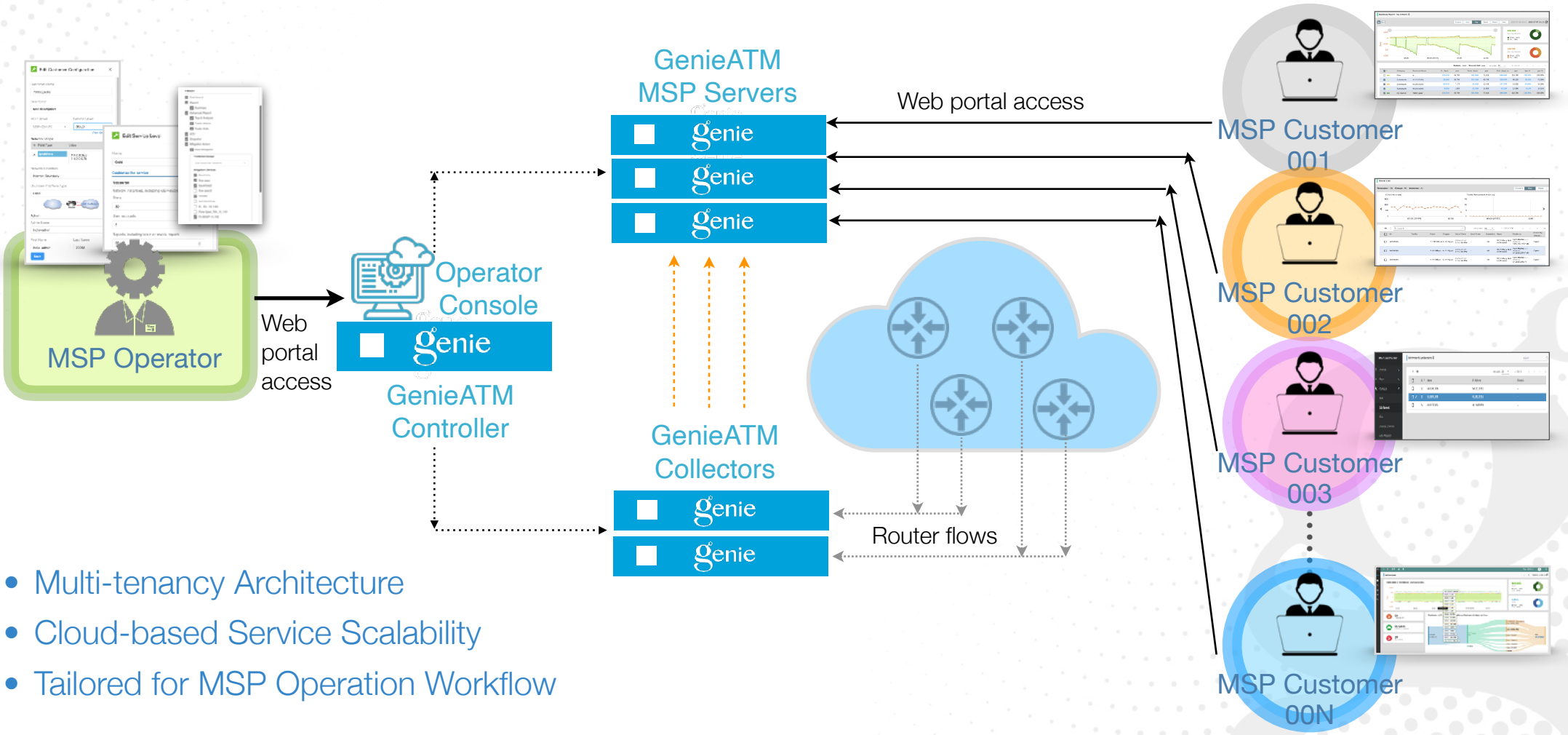
Instant troubleshooting tool & direct linkage to GenieAnalytics for attack forensics

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



- Multi-tenancy Architecture
- Cloud-based Service Scalability
- Tailored for MSP Operation Workflow

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

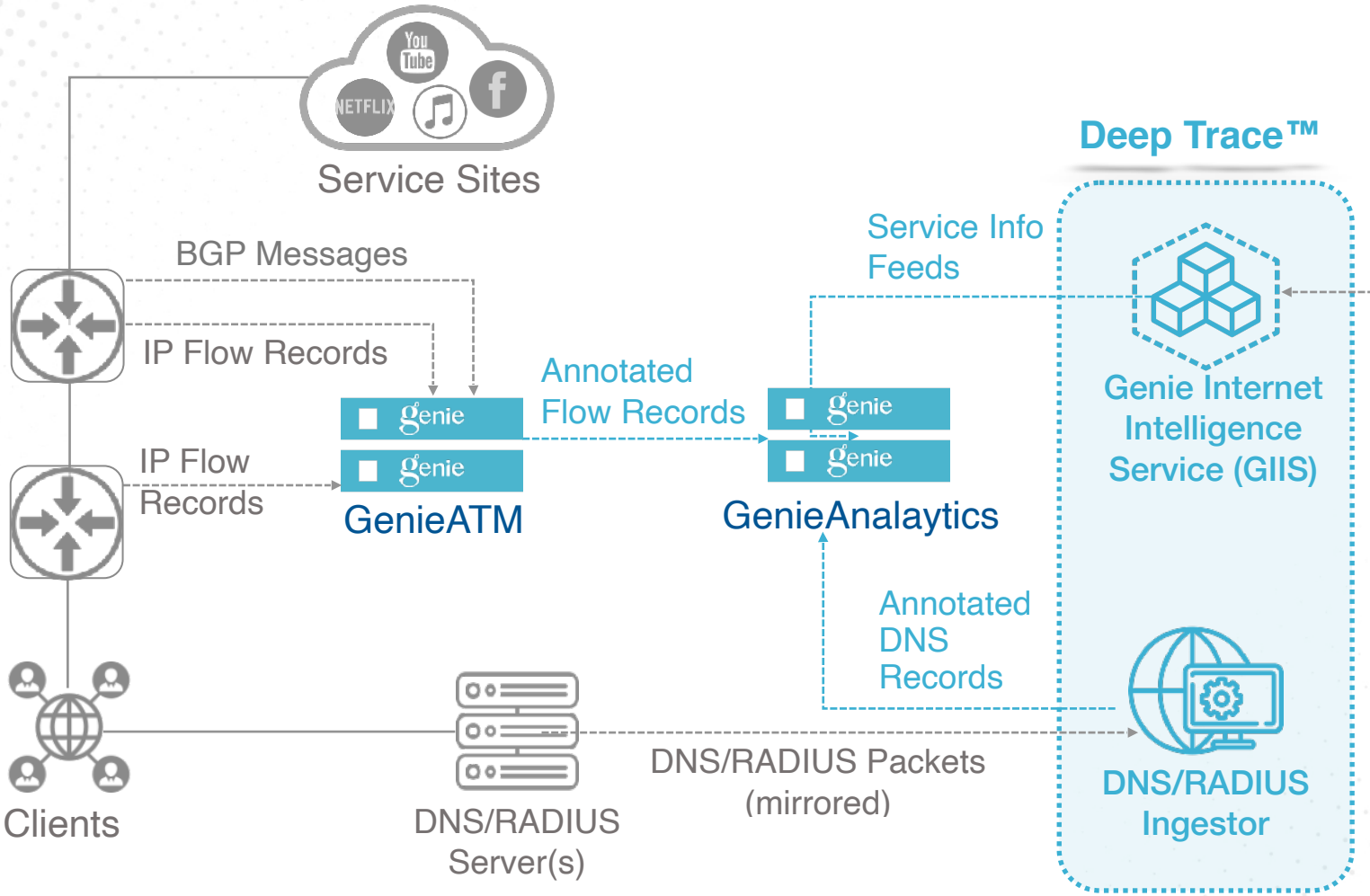
04 More Data Correlation

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



GenieATM

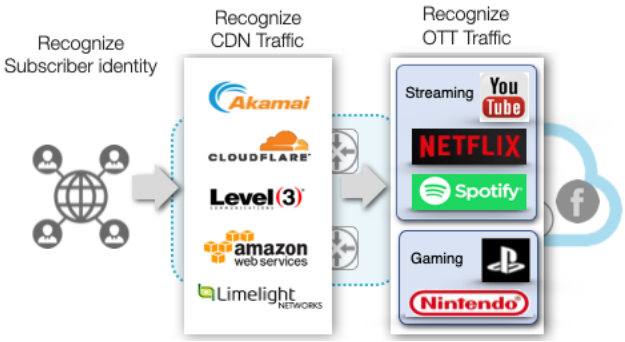
- Collects various data sources
- Correlates heterogeneous data and annotate flow data records

GA agent exports Annotated data records

GenieAnalytics

- Big data storage
- Multi-dimensional analytics
- Rich visualization

Powerful Big Data Analytics & Rich Visualization



Multi-dimensional Pipeline

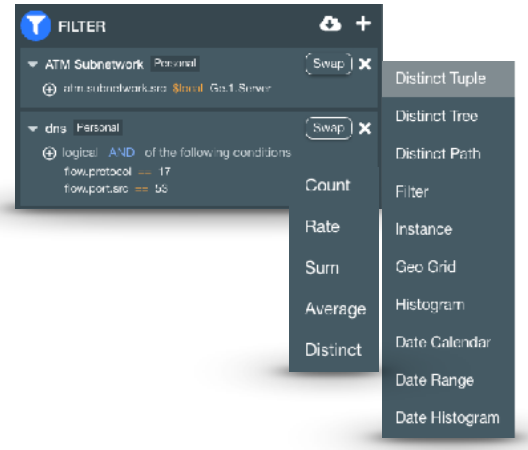
Interactive big data exploration with unlimited Filter combination and analytic aggregation keys.

Multi-tenant Architecture

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

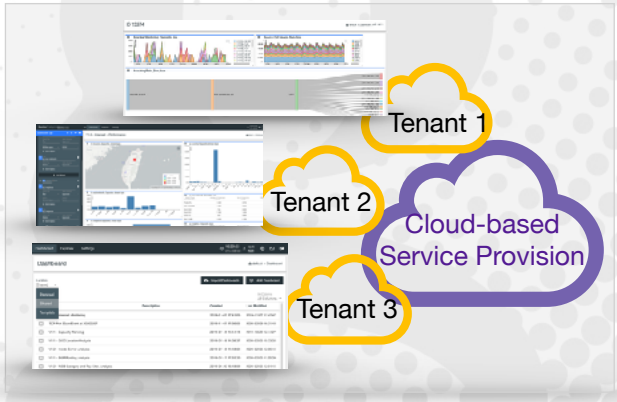
Enriched data

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

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

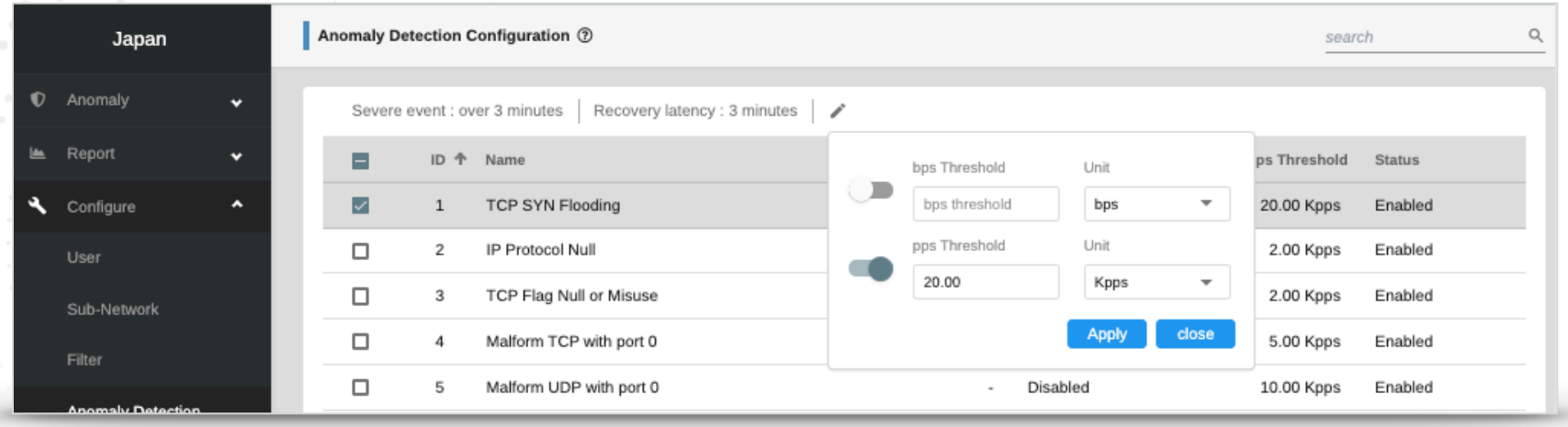
- Defend network-wide DDoS to protect its infrastructure
- A platform to easily enable managed services
- Carrier-grade performance, performance and reliability

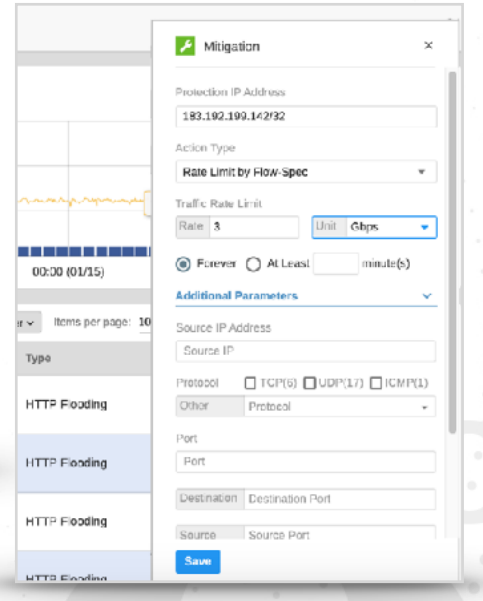
Why Genie

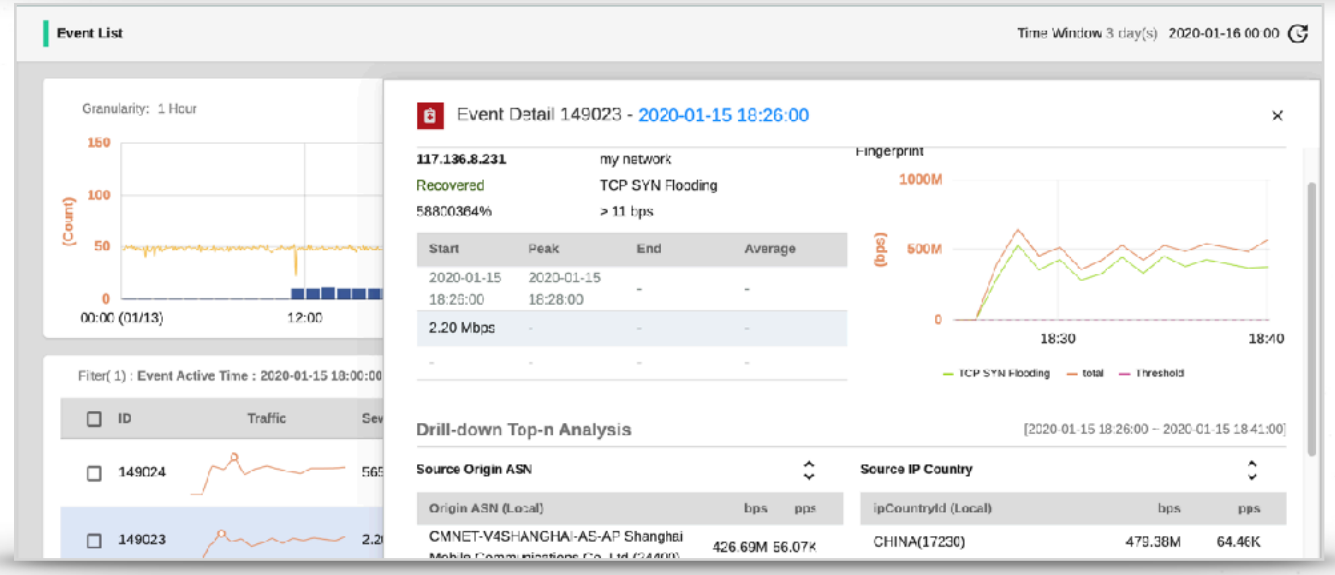
- A ready cost-effective, multi-tenant platform
- MSP business aligned workflow design
- Carrier-grade system scalability and high availability

Enabling MSSP Services

DDoS Security



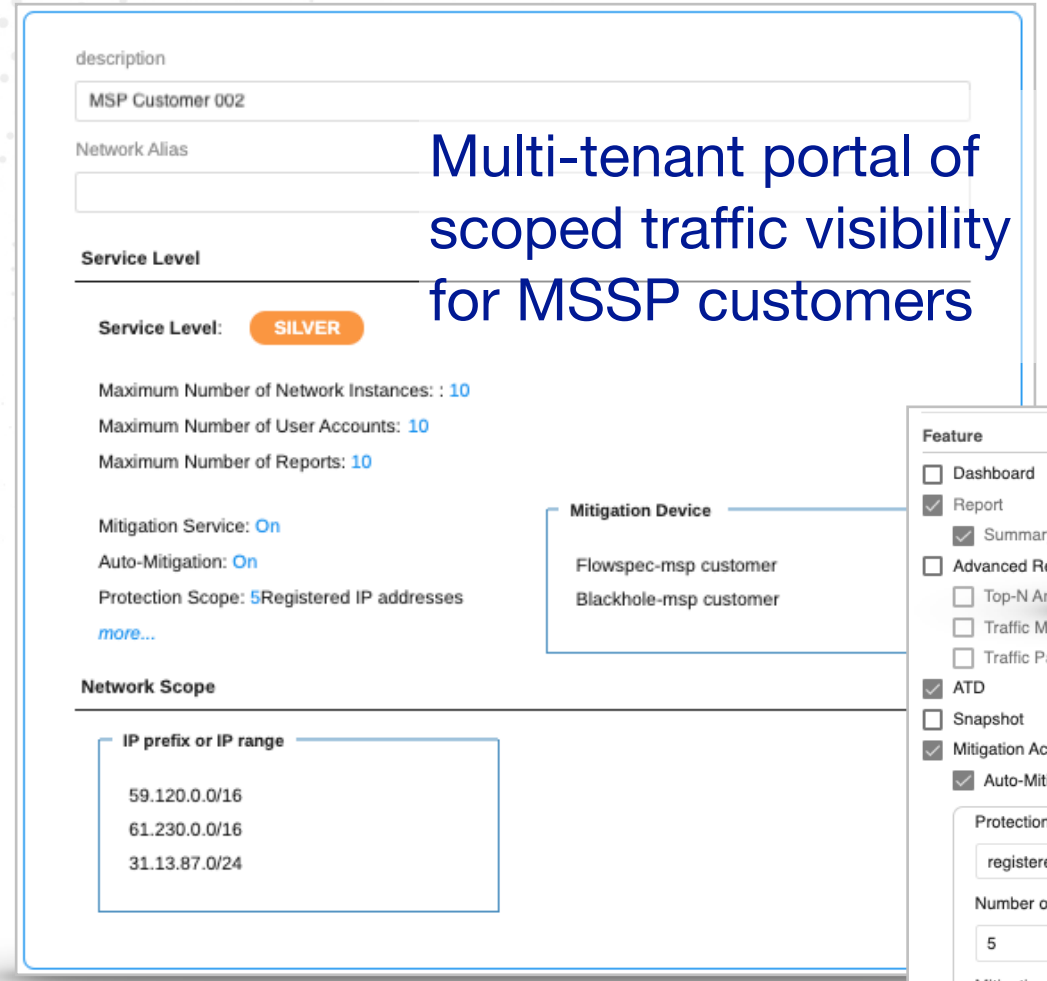


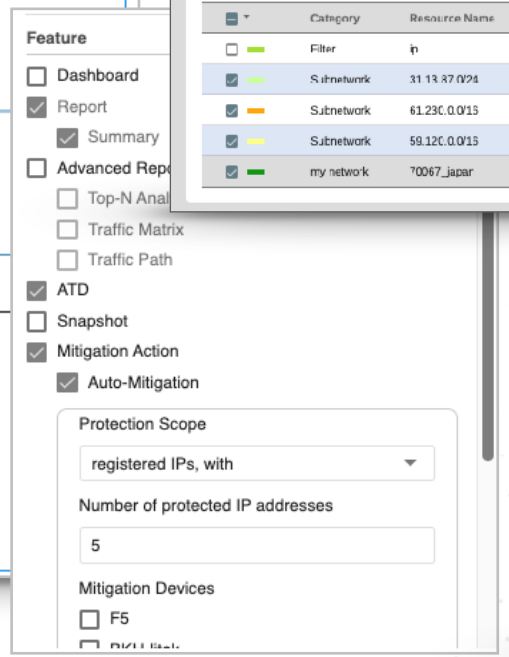


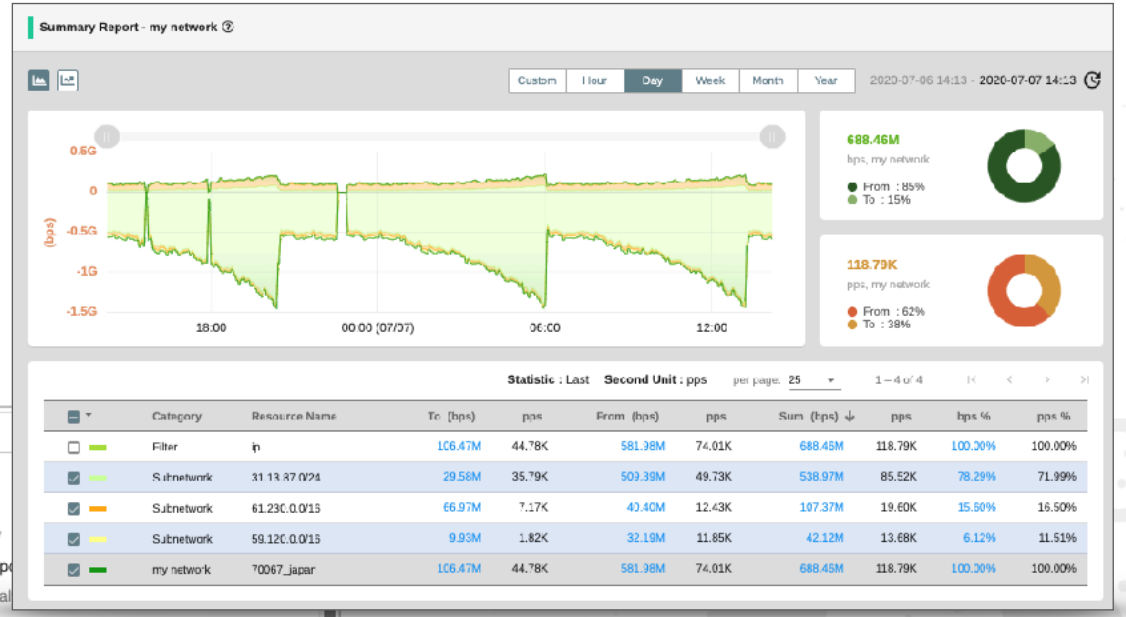
Multi-tenant detection & mitigation for each MSSP customer

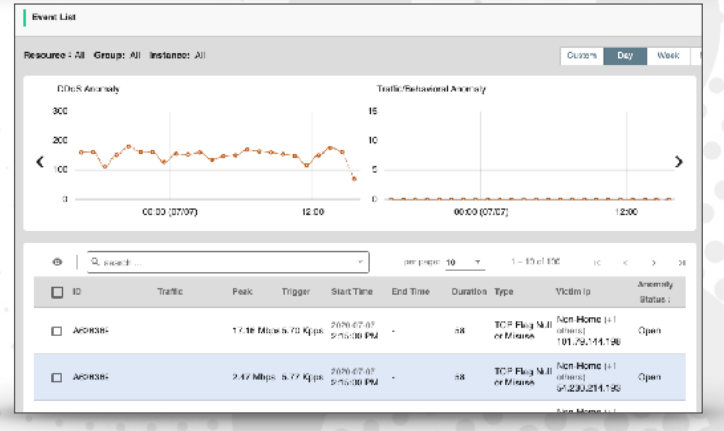
Enabling MSSP Services

Multi-tenant portal of scoped traffic visibility for MSSP customers









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-garde Solution

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

genie NETWORKS

THANK YOU!

www.genie-networks.com