CHINA TELECOM AMERICAS

DDoS Protection Services

EXPLORING
SUCCESS
TOGETHER

Legal Disclaimer

"The information contained in this presentation is provided for informational purposes only."

"The content of this presentation is proprietary information of China Telecom (Americas) Corporation. All intellectual property rights contained in this document, including but not limited to copyright, trademark, and tradename, are owned or licensed by China Telecom (Americas) Corporation or its affiliates."

Who is China Telecom (Americas) Corporation (CTA)?

China Telecom (Americas) Corporation (CTA) provides customized, cost-effective and integrated network and communication solutions to its diverse base of customers. As a leading facility-resale carrier with unique access to providers in Asia and the Americas, we offer a wide range of services such as direct internet access, internet transit, data services, data center, ICT services, mobile voice, professional services and industry solutions.

CTA is headquartered in Herndon, Virginia, with offices in Chicago, Dallas, Los Angeles, New York, Panama City, San Jose, Sao Paulo and Toronto. Enterprises throughout the Americas trust CTA's one-stop, turnkey solutions to meet the challenges of today's complex business environment.

Discover more at www.ctamericas.com

Who is China Telecom (Americas) Corporation (CTA)?

Established in 2001

250+
Employees in US, Canada & LATAM

7
Regional Sales & Support Offices

12
Points of Presence (PoPs) in South America

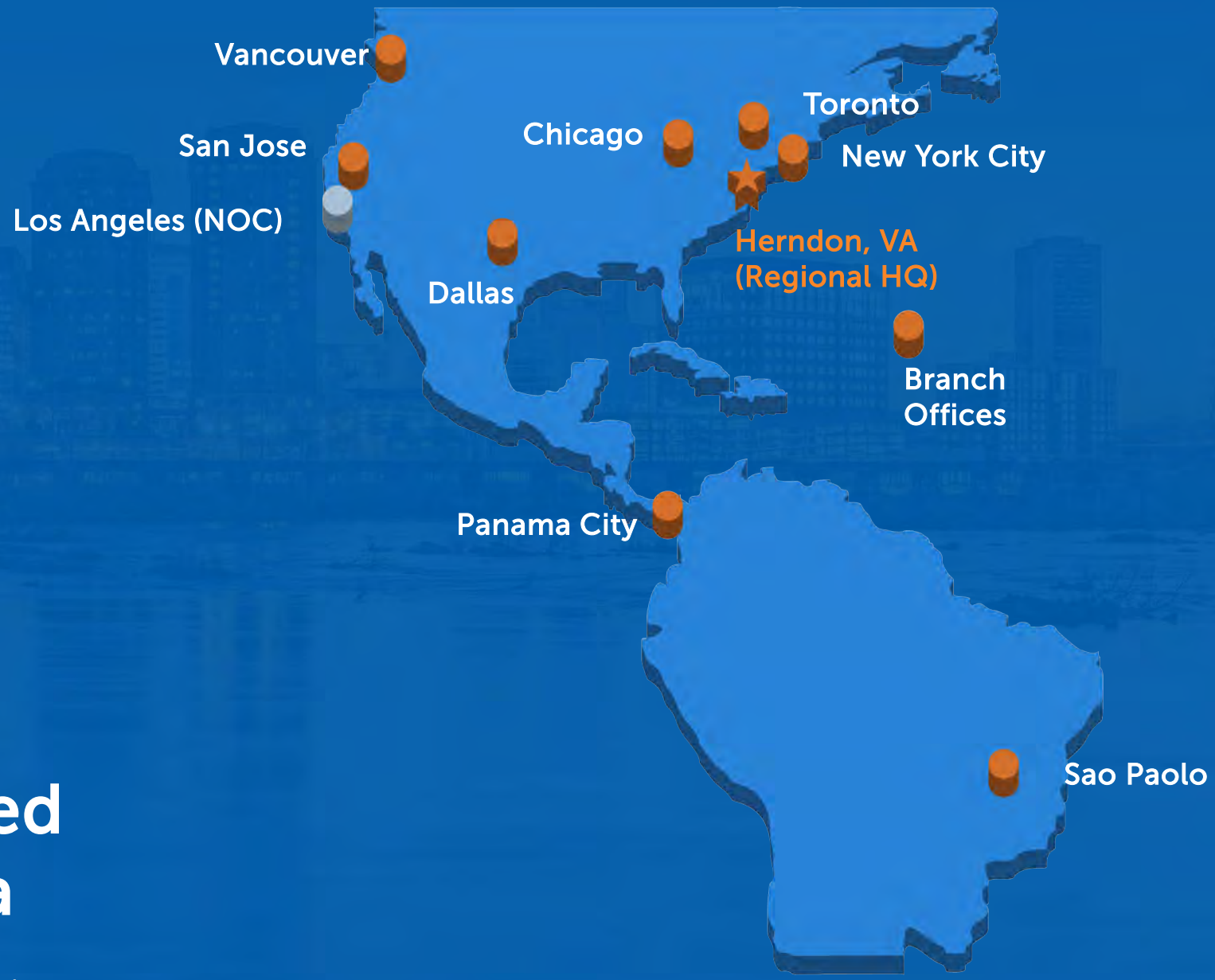
2
Network Operations Centers (NOCs) in LA & HK

22
Points of Presence (PoPs) in North America

21
Channel Master Partnerships

100+
Customers in the Fortune 500

100+
Carrier Partnerships



We have offices across America

CTA is headquartered in Herndon, Virginia

DDoS Attack

Distributed Denial of Service Attack (DDoS) is where hackers use two or more computers on the network as a "zombie botnet" to launch a "denial of service" attack on a specific target, so that the target computer's network or system resources become exhausted, and service is temporarily interrupted or stopped.

DDoS protection solutions prevent these kinds of attacks by monitoring web traffic and setting baselines for normal traffic loads. If an incoming traffic flow accelerates rapidly, web filters will identify abnormal events and redirect traffic to a controlled source.

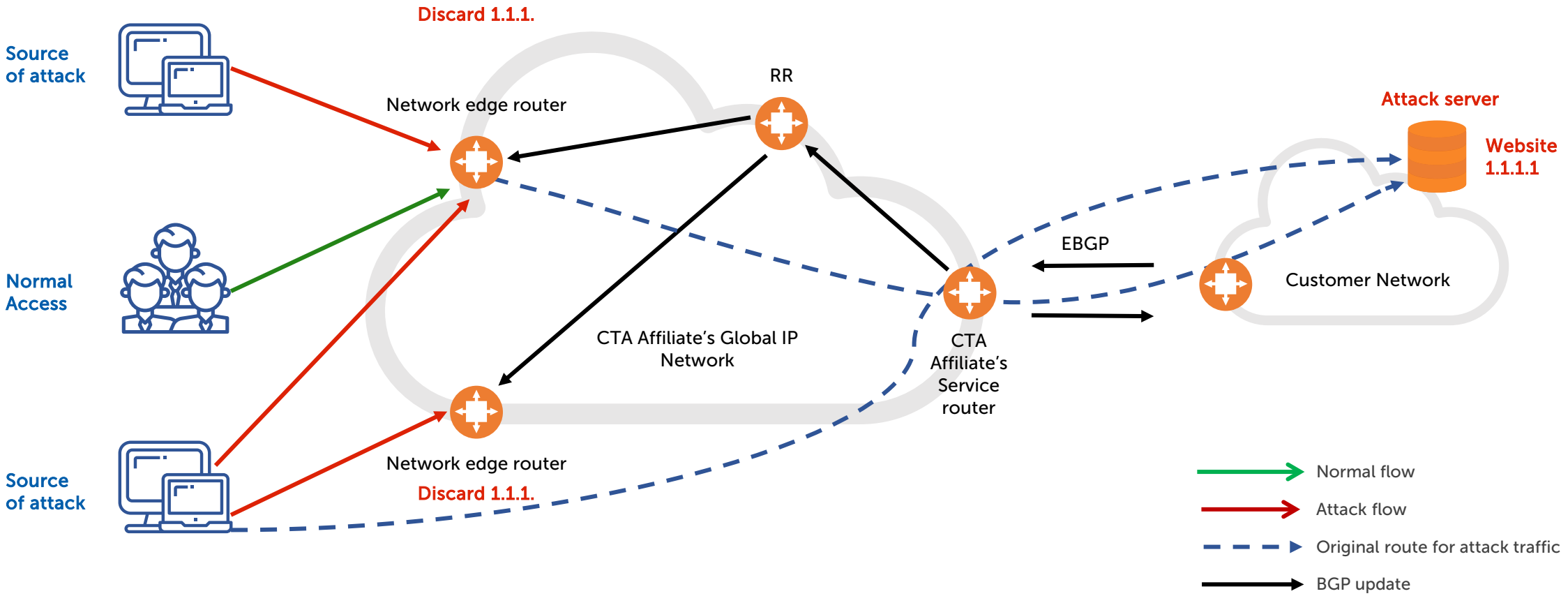
" DDoS attacks are the most dangerous cyber threat to every organization in the world "

DDoS Attacks are the Most Common Internet Security Threat

Impact of DDoS Attacks

- Lost Business Revenue & Partnerships
- Brand Loyalty & Reputational Loss
- Long-term Legal Impacts on the Business
- Unable To Access Critical Information
- Increased Cost of Restoring Services
- Lower Credit Ratings

Black-Hole Service Illustration



Clean-Pipe Service Illustration

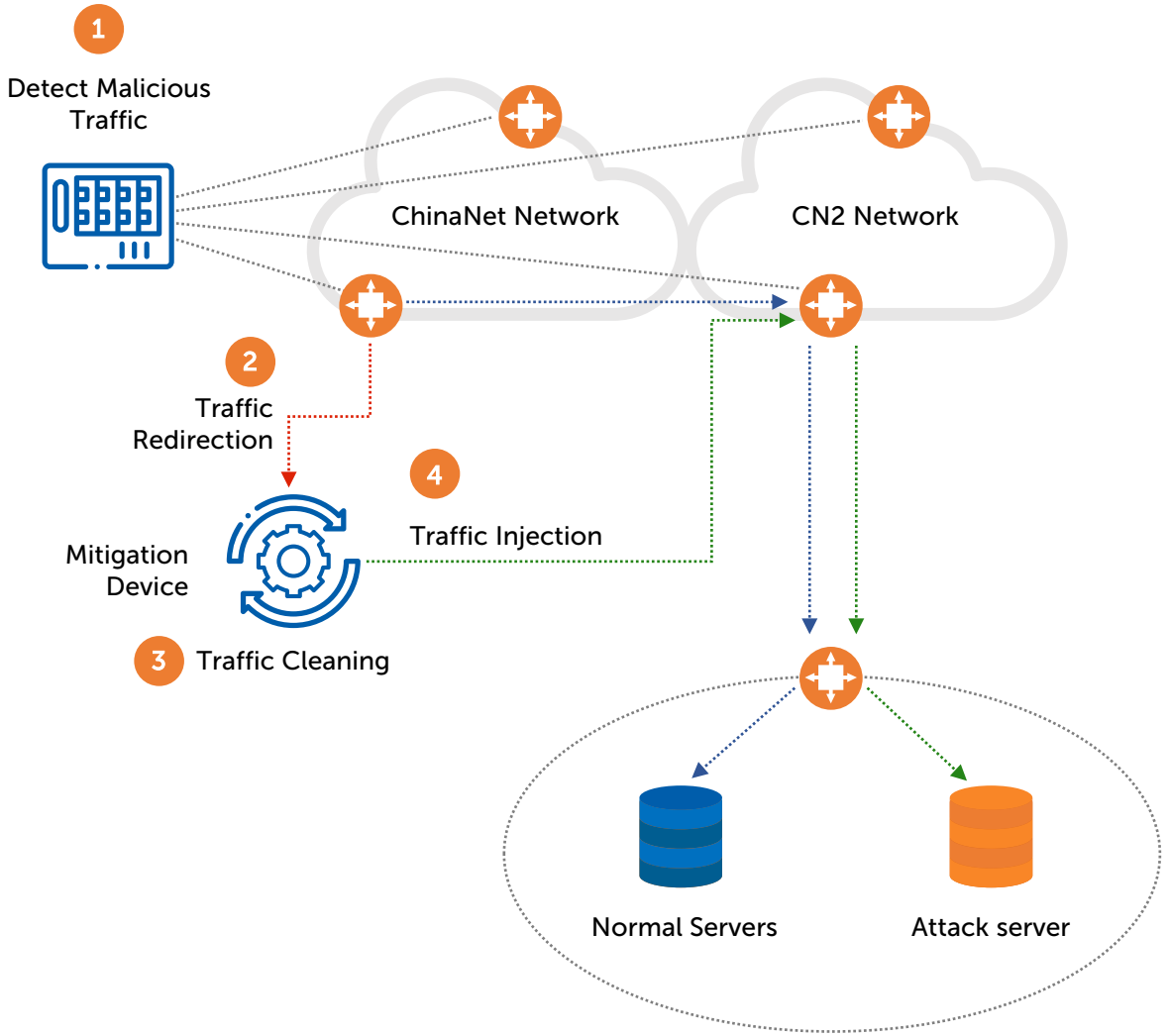
Real-time traffic monitoring of IP addresses that need to be protected. When an attack occurs, we uses the deployed dedicated mitigation platforms to re-route attack traffic, clean, and re-inject cleaned traffic back to the customer.

Monitoring and abnormal traffic detection.

Once a possible DDoS attack is detected, the mitigation device will announce a host route of the victim's IP address using BGP to divert traffic to the mitigation device.

The mitigation platform filters out the abnormal traffic as much as possible.

The filtered traffic sent back to the customer via CN2 network



Global Anti-DDoS Service

Bandwidth and service protection for customers who purchase Global Internet Service products.

Black-Hole Service

When DDoS attacks the user server, CTA changes the next hop of attacked target IP address to an empty address (or black-hole server) to block traffic and protect customer network.

Clean-Pipe Service

CTA provides real-time traffic monitoring of IP addresses customers need to be protected. When an attack occurs, CTA uses the deployed dedicated mitigation platforms to re-route attack traffic, clean at centralized scrubbing centers, and re-inject the cleaned traffic back to the customer.

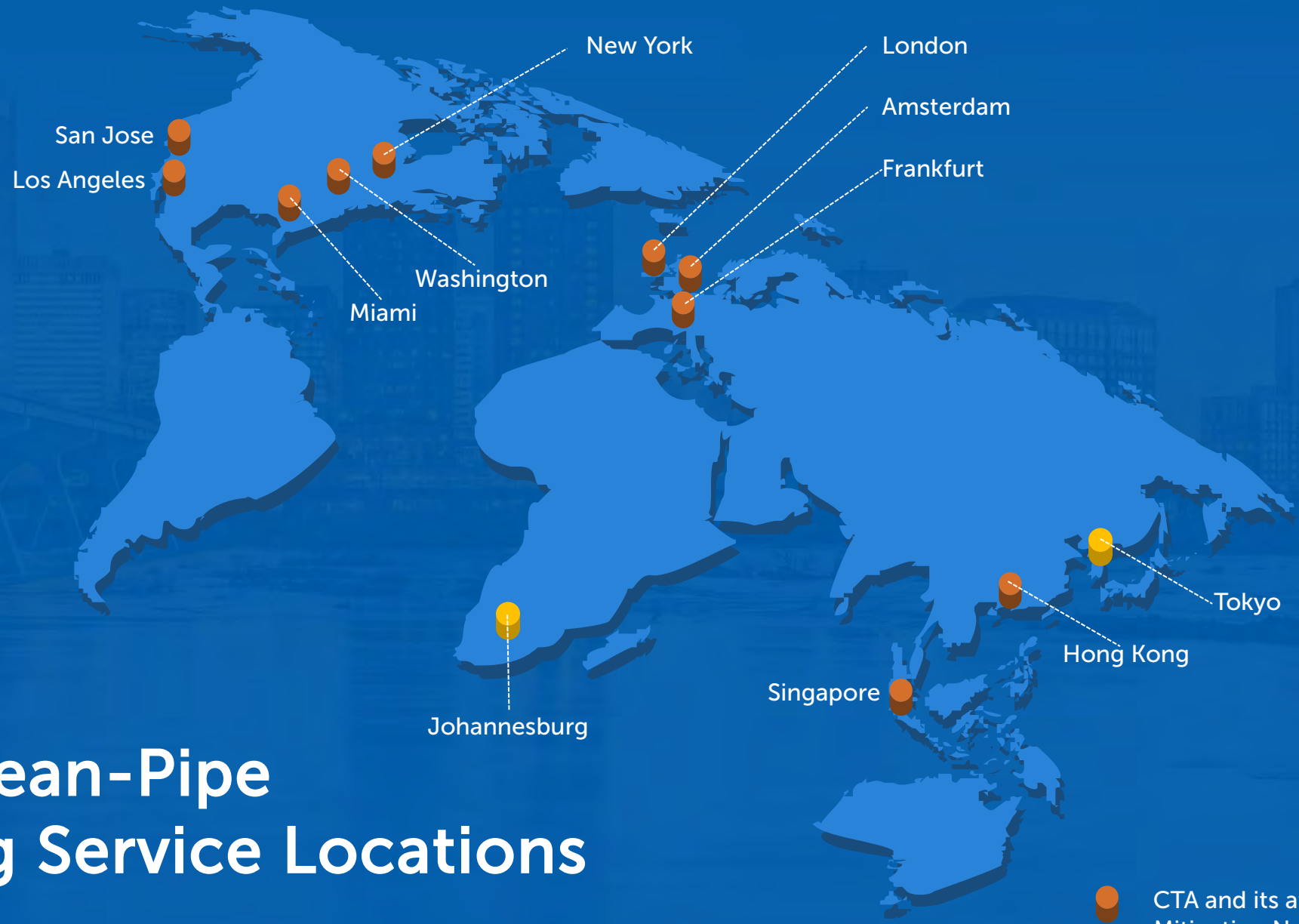
Global Black-Hole Service Implementation

BGP Community

- Service coverage for customers who access CN2 (AS 4809) network.
- Route Protocols via BGP Connection to the CN2 network (BGP community 4809:0).
- Effect of Black-Hole includes service interruption, including normal and attack traffic.
- Customer's Black-hole address must be /32 bit and White Listed.

Portal

- Service Coverage includes customers who access ChinaNet (AS 4134) or those who access CN2 (AS 4809) via static protocol.
- Portal Website http://ipms.chinatelecomglobal.com



Global Clean-Pipe Scrubbing Service Locations

CTA and its affiliates Mitigation Node

Under Construction

Global Clean-Pipe Service Features

Automatic Monitoring and Alerting

- Attack detection based on NetFlow
- TCP/IP (ISO Layer 3 & Layer 4) mitigation service
- Customer needs to nominate IP addresses to be protected by the service (Called “Managed Object”)
- Currently only provide mitigation for IPV4 addresses

Global Clean Pipe Service Guarantee

Service Support

CTA provides 24 x 7 Customer Service & Emergency Support

Mitigation Incident Initiation

The time from attack is detected and confirmation to traffic diverted into mitigation platform is done within 15 minutes.

Service Report

According to customer requirements, we can provide custom monthly service reports.

Mitigation Precision

DDoS detection and mitigation are operated on a best effort basis. We commit the mitigation precision for most type of DDoS.

China-Based DDoS Protection

Bandwidth

Total Network BW
More than 60000G

Ranked #1 in China

Capacity

26 Clean Centers Globally; More than 1000G Clean Capacity

Industry Leading

Professionalism

More than 1000 Experts

ISP level Expert Service

Timeliness

ISP Level fast response mechanism

Experience of National Security Projects

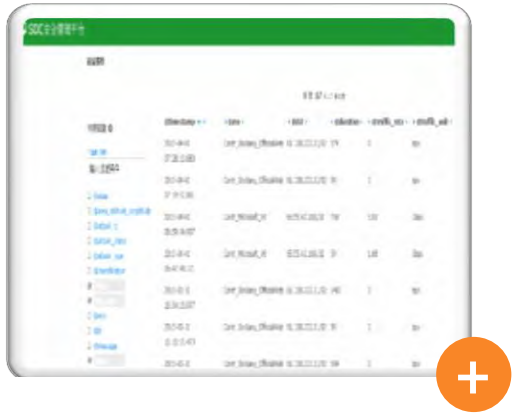
China Anti-DDoS Service Components

Automatic Monitoring & Alerting

Attack Protection & Near Source Mitigation

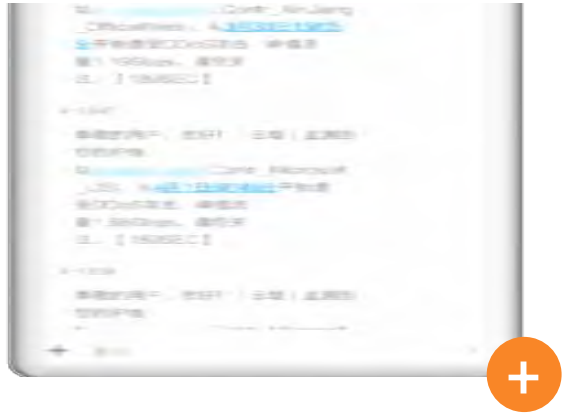
Comprehensive Attack Analysis & Reporting

Automated Monitoring and Alerting



1. Traffic collection statistics
2. Attack detection based on NetFlow
3. Sampling ratio (2000~5000:1)

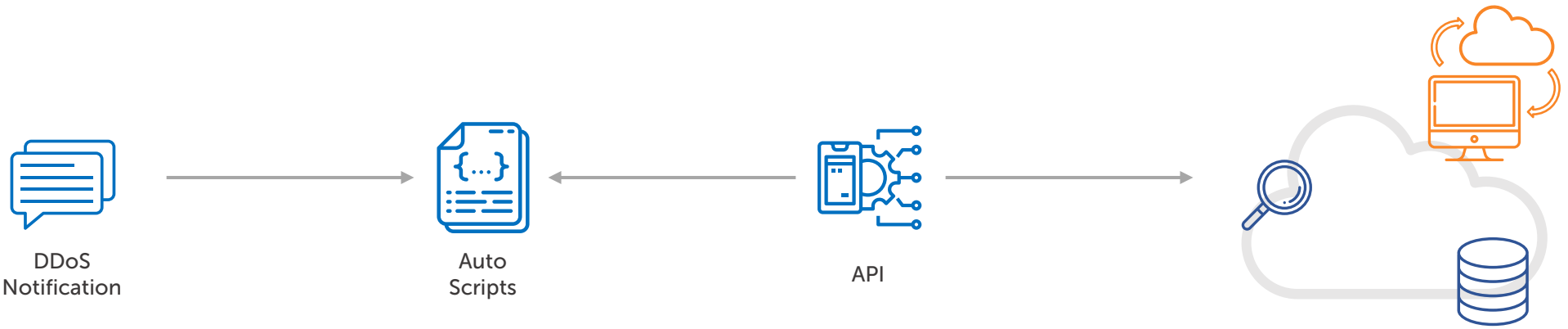
1. Real-time attack tracking and monitoring
2. Could target one customer's different IP segments; Or set the alert based on IP address



1. The system sends alter automatically.
2. Different options available including Text Message, WeChat, Email, Call, etc.

Traffic Mitigation

- Best Fit for Business Continuity Sensitive Customer
- Almost Zero Latency Added
- Automatically Triggered by Pre-configured Policy
- Zero Misidentification for Typical Attack



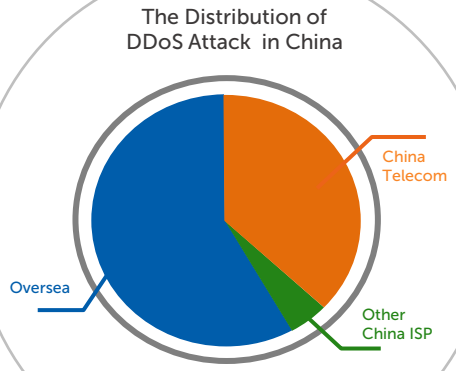
Comprehensive DDoS Attack Analysis

- Single Attack Analysis Report
- Tracking Attack and Analysis
- Monthly Analysis Report

Not Disturbed by False IP Address

Rank of DDoS Attack				
Targeted IP	Province	City	Start Time	Finish Time
183.61.*.*/32	GuangDong	Guang Zhou	11:27:19	11:58:52
115.238.*.*/32	ZheJiang	NingBo	14:39:48	15:02:57
115.238.*.*/32	ZheJiang	NingBo	11:27:41	11:57:52

Accurate tracking the attack, even located at local DC



Credible Analysis Results of DDoS Attack

Thank You

CHINA TELECOM AMERICAS

Contact Us or Visit:
ctamericas.com/coronavirus-support

To learn more about our offerings to support businesses during COVID-19.

607 Herndon Parkway, Suite 201
Herndon, VA 20170

marketing@ctamericas.com
www.ctamericas.com

EXPLORING
SUCCESS
TOGETHER

中国电信 CHINA TELECOM | FORTUNE GLOBAL 500 2018