Network Security
DDoS Attack Trend and Defense Strategy

Donny Chong, Product Director

NEXUSGUARD™

The Global Leader in DDoS Mitigation

NEXUSGUARD

Global Leader in DDoS Mitigation

#4
DDoS Top10Review

#24
CyberSecurityVenture
Top 500

FROST
&
SULLIVAN
Entrepreneurial Company 2016

8
Years experience
fighting DDoS

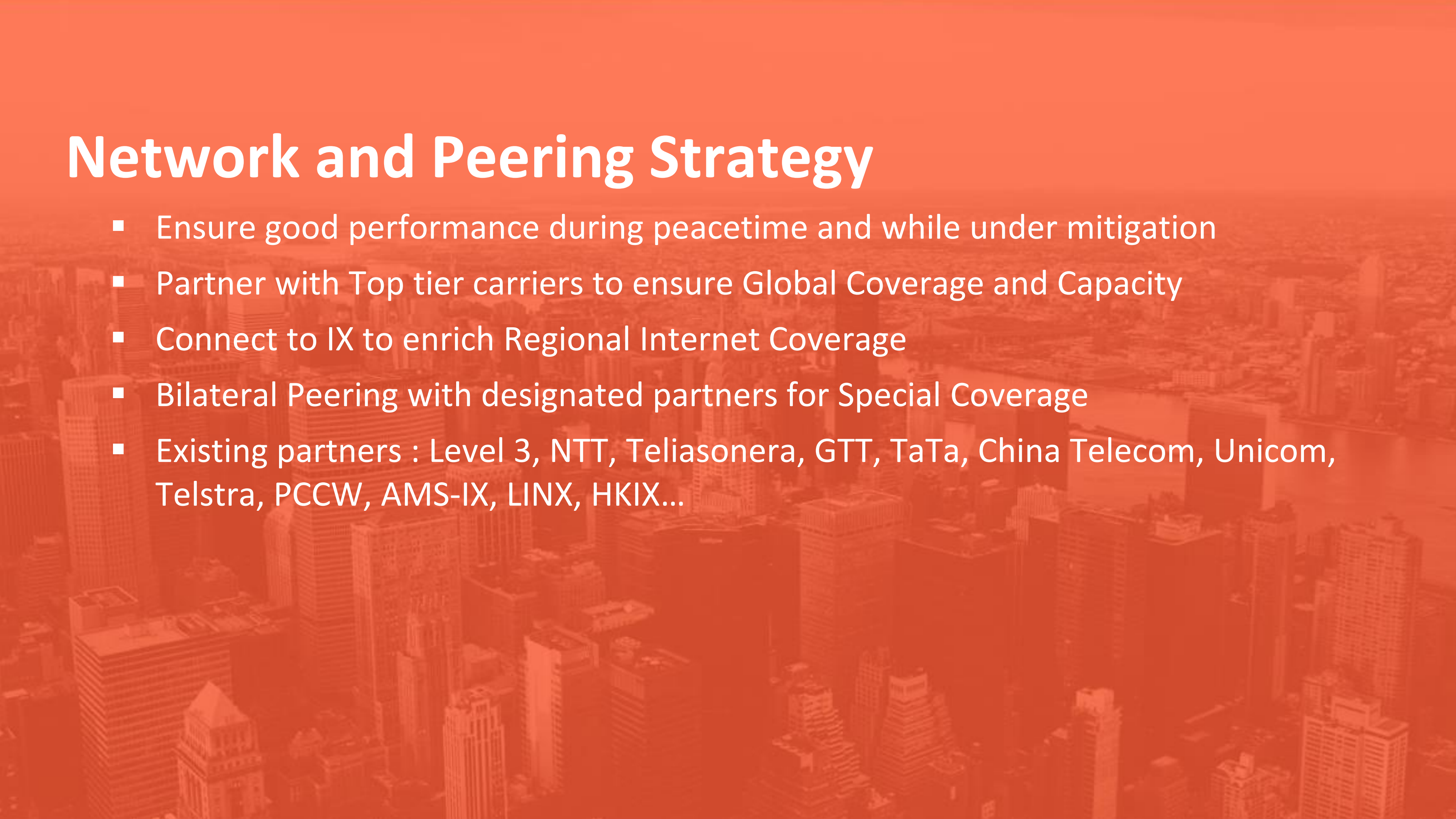
9
Global
Scrubbing Centers

1.44
Tbps
Scrubbing Capacity

24x7
Security Operation
Center

Pci
DSS
COMPLIANT
Service Provider Level 1

bsi.
ISO/IEC
27001
Information Security
Management



Network and Peering Strategy

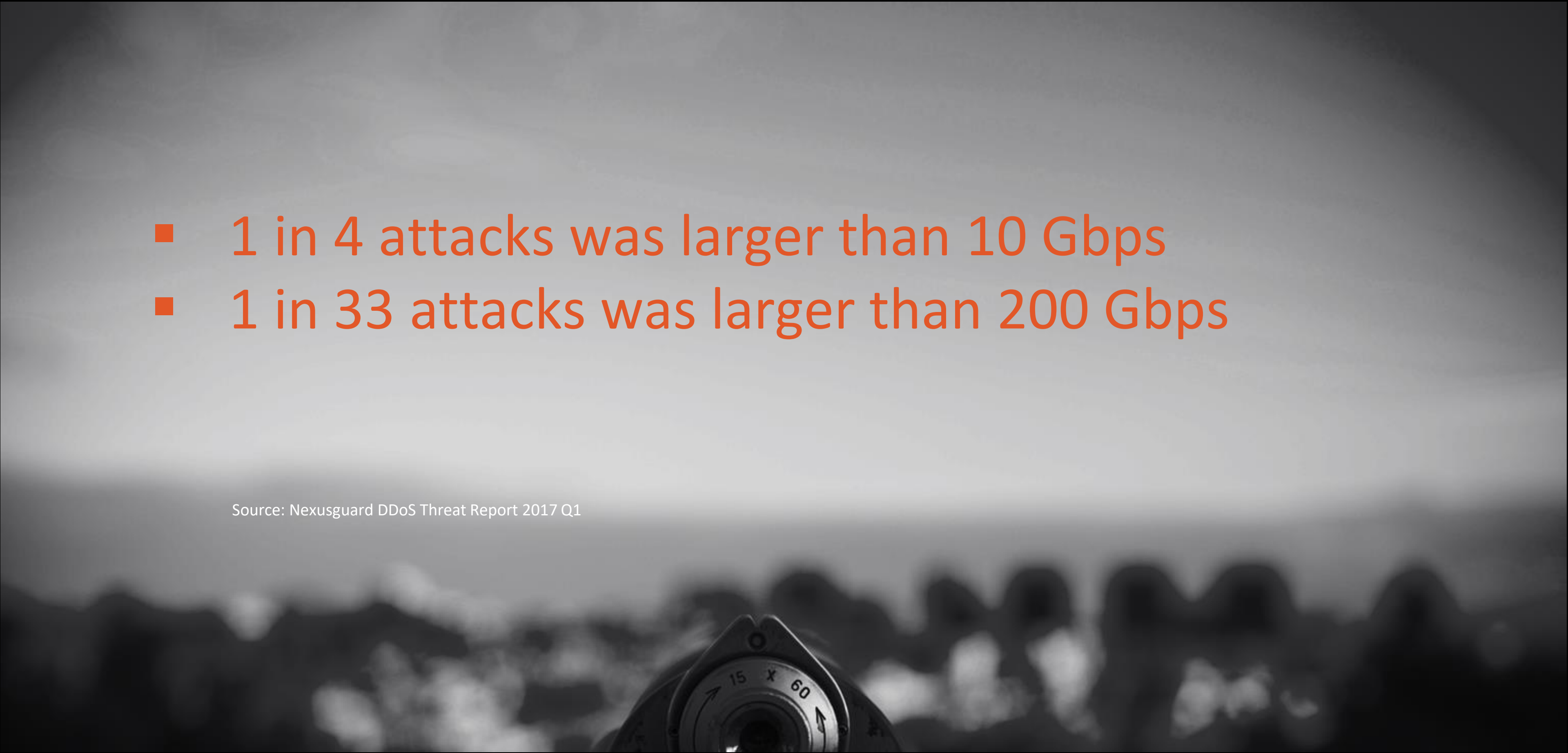
- Ensure good performance during peacetime and while under mitigation
- Partner with Top tier carriers to ensure Global Coverage and Capacity
- Connect to IX to enrich Regional Internet Coverage
- Bilateral Peering with designated partners for Special Coverage
- Existing partners : Level 3, NTT, Teliasonera, GTT, TaTa, China Telecom, Unicom, Telstra, PCCW, AMS-IX, LINX, HKIX…

Recent trends

- Attacks have become larger in size, longer in duration, more complex in attack techniques, and more frequent than ever
- IoT devices and industrial IoT systems will play a bigger role in DDoS attacks
- Layer 7 attacks are much more common now, especially HTTP GET floods
- Multi-vector attacks are on the rise
- DDoS attacks increasingly being used as smokescreen to cover up other cybercrimes

Some Observations in 2017 Q1

Source: Nexusguard DDoS Threat Report 2017 Q1



- 1 in 4 attacks was larger than 10 Gbps
- 1 in 33 attacks was larger than 200 Gbps

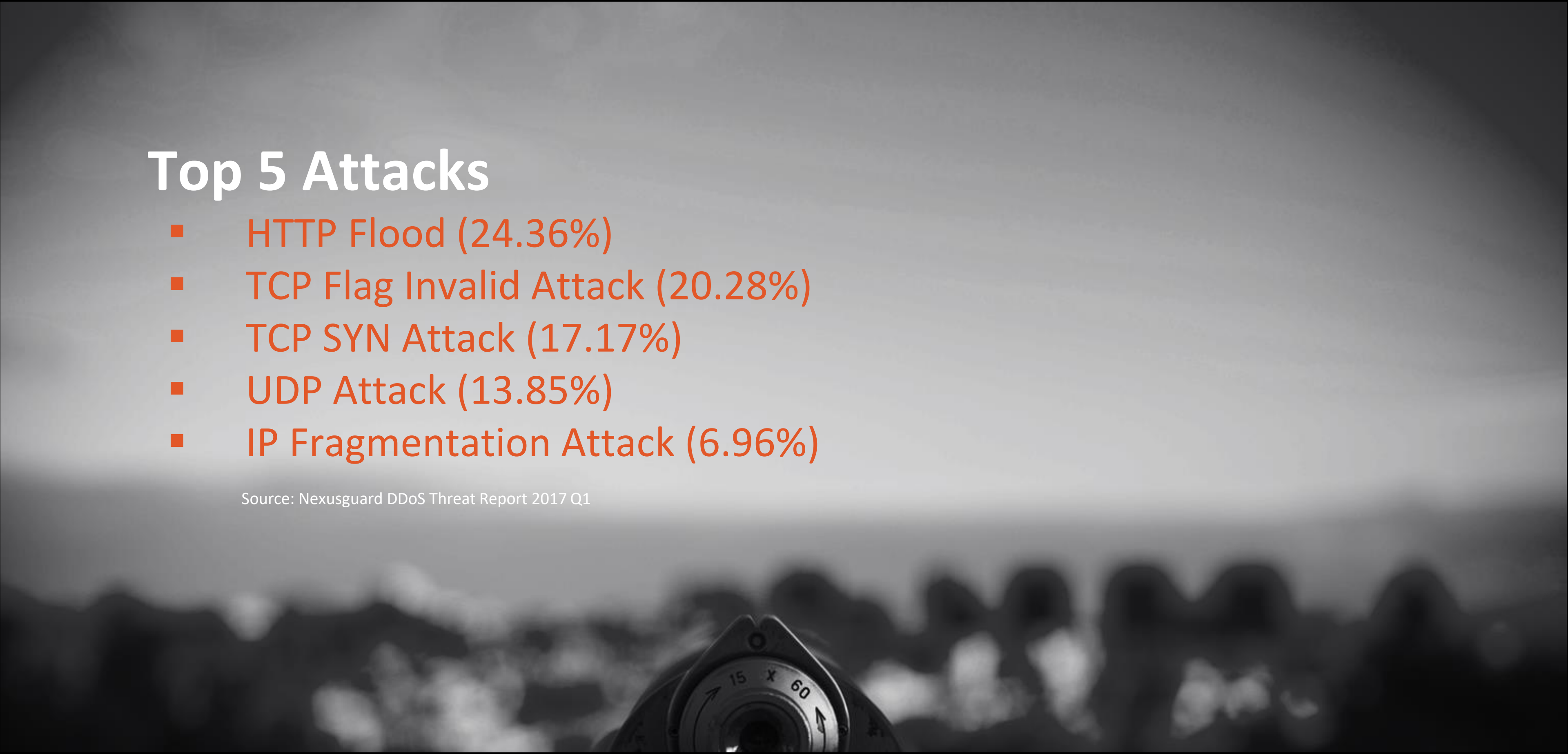
Source: Nexusguard DDoS Threat Report 2017 Q1

- 68% were multi-vector attack
- The Most complicated one contained 10 attack vectors

Source: Nexusguard DDoS Threat Report 2017 Q1

- 48% attacks lasted for 90+ minutes
- The Longest one lasted for 2d19h40m

Source: Nexusguard DDoS Threat Report 2017 Q1



Top 5 Attacks

- HTTP Flood (24.36%)
- TCP Flag Invalid Attack (20.28%)
- TCP SYN Attack (17.17%)
- UDP Attack (13.85%)
- IP Fragmentation Attack (6.96%)

Source: Nexusguard DDoS Threat Report 2017 Q1

Attacks have become larger, longer and more complicated

What is the Challenge for Service Provider?

Challenge

Internal

Tools
to handle multi vector attack

People
Skill, team & Workflow

Intelligence
Up-to-dated attack trend and defense strategy

Process
Detection> Mitigation> Reporting

Customer

Customized Requirement

24/7 Mitigation and Recovery

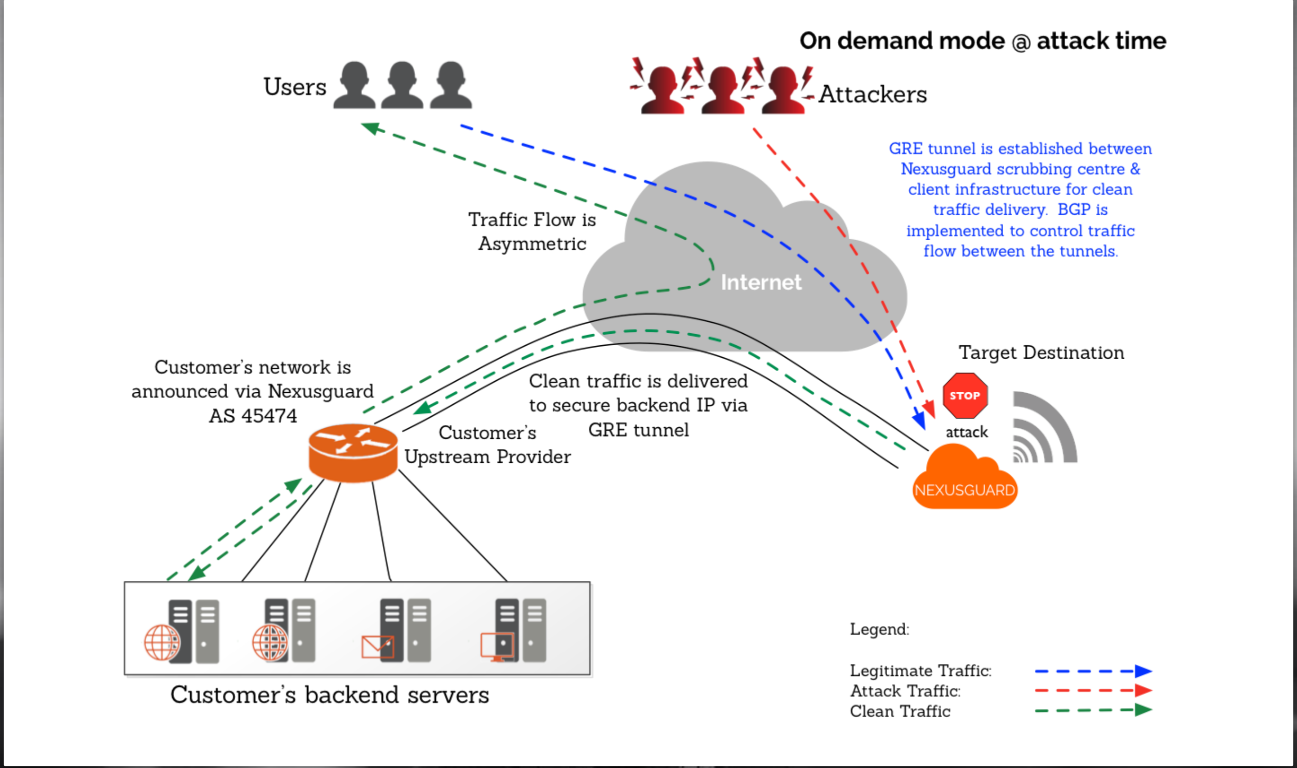
Collateral Damage

Incident Report

Case Study

Category	Attack Type	
Bandwidth/ Network Depletion Attacks	Protocol Flood/ Exploitation Attacks	TCP Flood, UDP Flood, ICMP Flood, TCP SYN, SYN/ACK, RST, FIN Flood, IP Null, Fragmentation, DNS Amplification, Fraggle, Nuke, TCP Flag Abuse, Zombie/ Bots Attack
Application-based Attacks	HTTP Attacks	HTTP GET/POST Flood, HTTP PAGE Flood, HTTP Connection Flood, HTTP Malformed Request, HTTP 404, Slowloris, Socketstress, Slow HTTP
	DNS Attacks	Reflected DNS, DNS Query, DNS UDP Flood, DNS TCP Flood, DNS Malformed Query, Protocol and Vulnerability Exploitation DoS/DDoS
	Hacks	SQL injection, Cross Site Scripting (XSS), Cross Site Request Forgery (XSRF), Session Hijack
Others		Malicious Headers, Malicious Payloads, Pucodex, Zero Day Exploits

When Attacks come



On demand mode @ attack time

Users
Attackers
Internet
Traffic Flow is Asymmetric
Target Destination
STOP
attack
NEXUSGUARD
Customer's Upstream Provider
Customer's backend servers

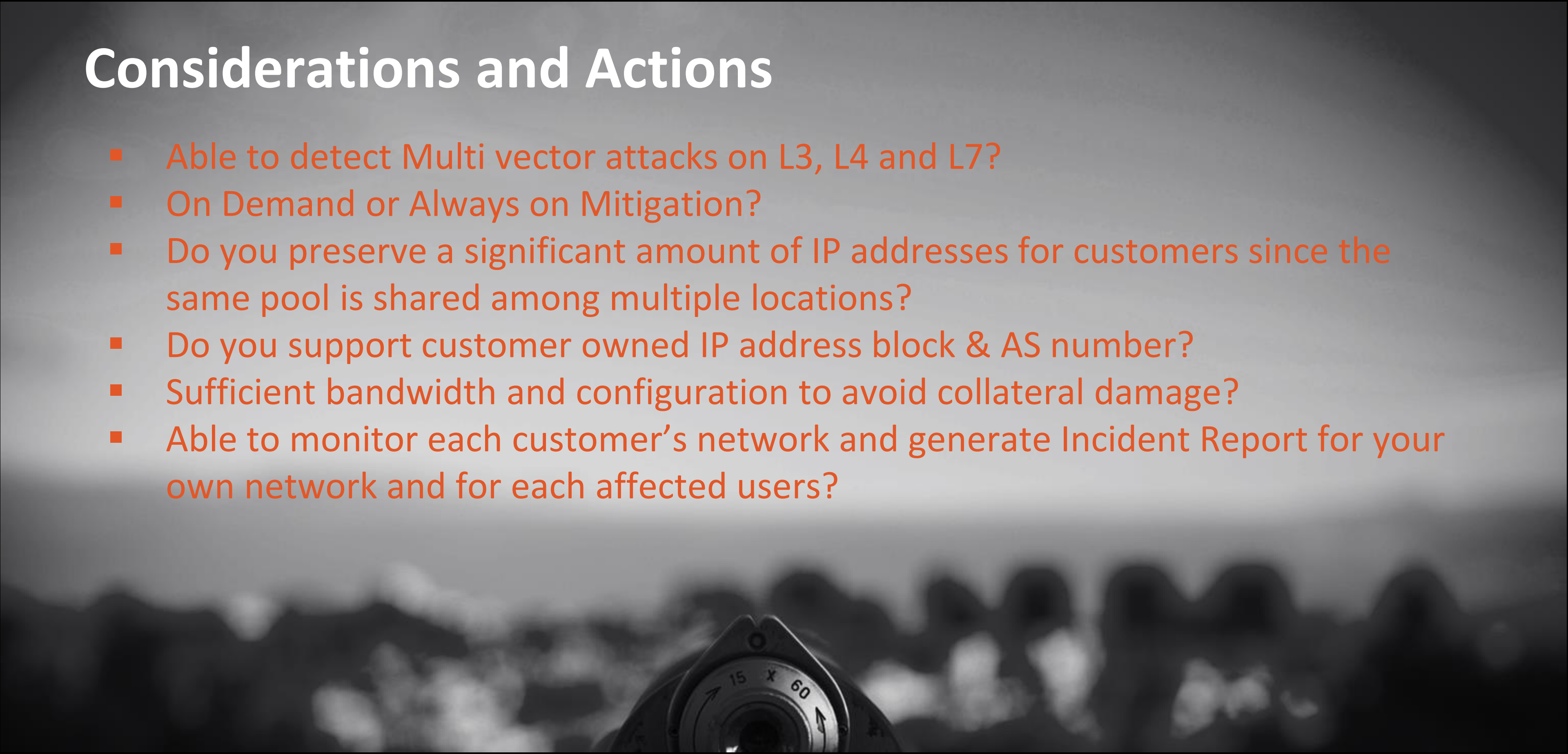
GRE tunnel is established between Nexusguard scrubbing centre & client infrastructure for clean traffic delivery. BGP is implemented to control traffic flow between the tunnels.

Customer's network is announced via Nexusguard AS 45474

Clean traffic is delivered to secure backend IP via GRE tunnel

Legend:

Legitimate Traffic:	🟦 - - - ▶
Attack Traffic:	🟥 - - - ▶
Clean Traffic	🟩 - - - ▶



Considerations and Actions

- Able to detect Multi vector attacks on L3, L4 and L7?
- On Demand or Always on Mitigation?
- Do you preserve a significant amount of IP addresses for customers since the same pool is shared among multiple locations?
- Do you support customer owned IP address block & AS number?
- Sufficient bandwidth and configuration to avoid collateral damage?
- Able to monitor each customer's network and generate Incident Report for your own network and for each affected users?

Key benefits

- Global scrubbing network capable of protecting network infrastructure
- 24x7x365 monitoring, attack mitigation and incident response by SOC
- Full network traffic visibility, advanced analytics and real-time threat detection for all traffic
- Multilevel, customizable mitigation policies for ease of managing vast networks, such as those managing hundreds of Class C networks or a Class B
- DDoS expertise, technical support and threat intelligence
- No Capex, very low Opex

Data Sovereignty

In some jurisdictions and specific industries such as the FSI, data sovereignty is of utmost importance to service providers and enterprise organizations. Data must be managed and controlled according to the various laws, rules and regulations of each industry and country -- and different countries demand something different from an organization.

One barrier to adopting cloud-based security solutions is the compliance of data sovereignty laws. Enterprises work in so many different locations and with so many different vendors that it becomes difficult to guarantee the data sovereignty of information.

Nexusguard’s Service Provider Enablement (SPE) solution includes a hybrid deployment model that combines on-premise and cloud mitigation, which is ideally suited for customer environments that demand extremely low latency and multi-layered protection while complying with local data sovereignty laws.
Nexusguard itself is a PCI certified service provider (Level 1) guaranteed with the capabilities to process, store and transmit credit card data and sensitive information on our infrastructure, which is also PCI DSS3.0 compliant, including all data centers responsible for delivering the specific services.
Enterprise clients can request for traffic to be routed to a particular data center of their choosing in order to comply with local data sovereignty laws.
Nexusguard’s data centers are physically located in San Jose, CA; Los Angeles, CA; Miami, FL; Ashburn, VA; London; Amsterdam; Singapore; Taiwan; and Hong Kong.
Nexusguard has an SSL Key Management tool to look after the private key of enterprise clients securely. For those who cannot turn over their private key to a third party because of regulatory requirements, we can also utilize a Multi-Domain SSL Certificate solution to handle and mitigate SSL-encrypted traffic.

A sound DDoS Protection doesn’t only protect your customer and you

It delivers value and gains trust
It creates new business opportunity and revenue for your company!

Mr. Donny Chong
Product Director
donny.chong@nexusguard.com

NEXUSGUARD™
Global Leader in DDoS Mitigation