

NEXUSGUARD®

DDoS Protection Made Simple

AFR-IX
telecom

Simplifying DDoS

For Service Providers



NEXUSGUARD®

DDoS Protection Made Simple



Cybersec Asia Award
Best DDoS Defense 2020 - 2023



Technology Leader
DDoS Mitigation Global Market
2017 - 2023



Rising Star Partner
of the year 2022



Top 10 leading vendor
Asia-Pacific DDoS Solutions
Growth Opportunities 2021



Sample Vendor
Hype Cycle for Network Security -
DDoS Defense



Representative Vendor
Market Guide for
DDoS Mitigation Services



Best Security-As-A-Service
Information Management Awards
2018



Strong Performer
The Forrester Wave™
DDoS Mitigation Solutions 2017

15

Years experience
fighting DDoS since 2008

56

Global
DDoS Scrubbing Centers

3

Tbps
Scrubbing Capacity

24x7

Security
Operation Center



PCI DSS Compliant



ISO 27001 Compliant



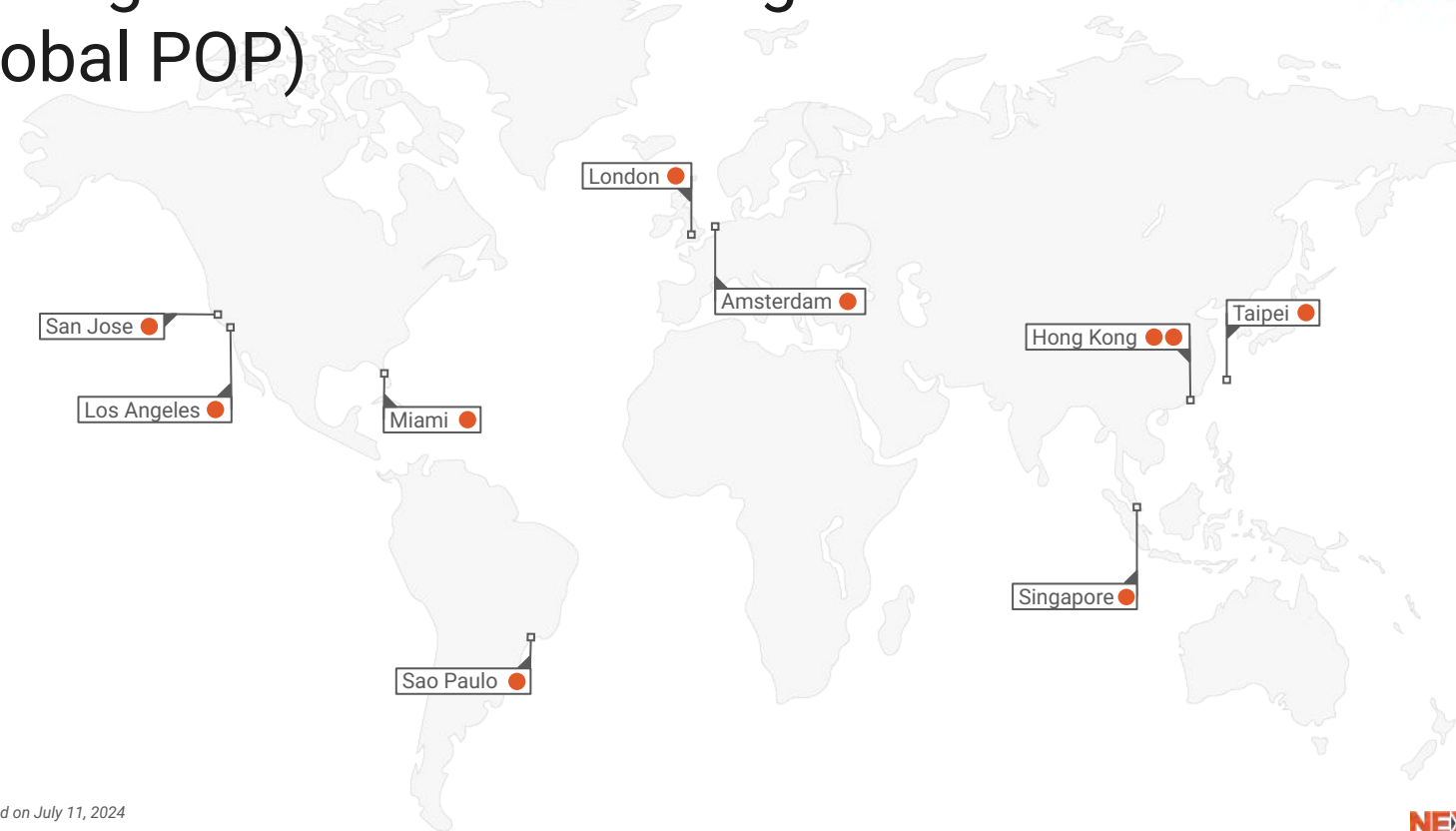
SOC Type 2 Compliant



Meta Threat Exchange Member

NEXUSGUARD®

Nexusguard DDoS Scrubbing Network (Global POP)



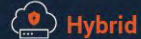
Last updated on July 11, 2024

MANAGED PROTECTION

Simplified Managed DDoS Protection for ISPs



- 24x7 Monitoring
- Layer 3-7 Protection
- Auto Diversion
- Fully Managed



- On-premise Appliance
- Unlimited Attacks
- Global DDoS Mitigation Network
- Lowest Latency

PARTNER PRODUCTIZATION

ISPs that desire to sell Managed DDoS Services



- 15 Days to Deploy
- Resell DDoS/ WAF Protection
- No Hardware Required
- Co-branded Multi-Tenant Portal



- 90 Days to Deploy
- Clean Pipe Protection for Internet Services
- Fully Managed On-premise Appliance
- Training/ Certification



Our Products

DDoS Protection

On-premise Bastions Server and Service

Nexusguard Bastions server is a powerful, versatile "cloud-in-a-box" deployment that seamlessly integrates Nexusguard's proprietary technologies and global cloud scrubbing into a modular chassis built into the CSP's environment.

- Bastions Server
- Clean Pipe (L3, L4)
- Network Protection (L3, L4)

Managed Cloud Based Protection

leveraging on our highly scalable, fully redundant and globally distributed scrubbing network to mitigate the largest and most sophisticated DDoS attacks.

- Application Protection (L3, L4, L7)
- DNS Protection (L3, L4, L7)
- Origin Protection (L3, L4)
- Edge Protection (L3, L4)



Productization & Enablement

Transformational Alliance Partner (TAP)

The TAP program provides customized, cost-effective DDoS protection solutions for CSPs, protecting the core infrastructure while meeting customer demand for comprehensive DDoS protection.

- Anti-DDoS Service Productization
- Sales & Marketing GTM support
- Co-branded option

Nexusguard Academy

Courses created and delivered by practitioners to equip CSP staffs with real-world, executable skills and knowledge to lead their organization on its part of transformation and towards success.

- Nexusguard Certified Pentester
- Nexusguard Certified Incident Responder
- Nexusguard Certified Security Associate
- Information Security Management System

DDoS Protection SIMPLIFIED



PROTECTION

We have Simplified Managed DDoS Protection for ISPs into two offerings to meet your needs and budget.

PRODUCTIZATION

For ISPs that desire to sell Managed DDoS Services we have two partner programs: Cloud resale and integrated partner.

Cloud-Based

- 24x7 Monitoring
- Custom Profiles
- Auto Diversion
- Unlimited Attacks
- Full or Co-Managed
- BGP Peering
- GRE Tunnel / Direct

Protection



Partner Program



Cloud Partner

- DDoS /WAF /DNS
- Website Protection
- Lowest Investment
- 15 Days to Deploy
- No Hardware
- Co- Label
- Multi-Tenant Portal

True Hybrid

- On-Premise Appliance
- Host Level Diversion
- Global Profile Sync
- Data Sovereignty
- Lowest Latency



True Hybrid TAP Partner

- Clean Pipe
- Application Protection
- DDoS / WAF / DNS
- 90 Days to Deploy
- Dell Server On-Site
- Training / Certification

4 Pillars

- Clean Pipe
- Application Protection
- Origin Protection
- DNS Protection

Maximising Cyber Services with Different Customer Segments

Nexusguard 4 Pillar Services



Layer 7

Application

Application Protection

- Reverse Proxy
- Always-on
- SSL offloading
- WAF
- Cache
- Load Balancing

- Support for other Telco customer

DNS Protection

- Reflected DNS, DNS Query
- DNS UDP Flood, DNS TCP Flood
- DNS Malformed Query
- Protocol and Vulnerability Exploitation DoS/DDoS
- Support for other Telco

Layer 3, 4

Network & Transport

Origin Protection

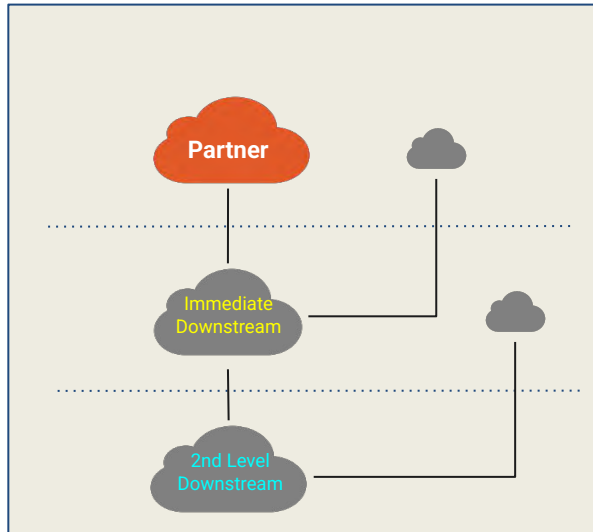
- BGP swing
- Always-on / On-demand
- Class C & AS#
- NetFlow, GRE
- Support for other Telco

Clean Pipe Protection

- Telco DIA
- Always-on
- Public / Private IP

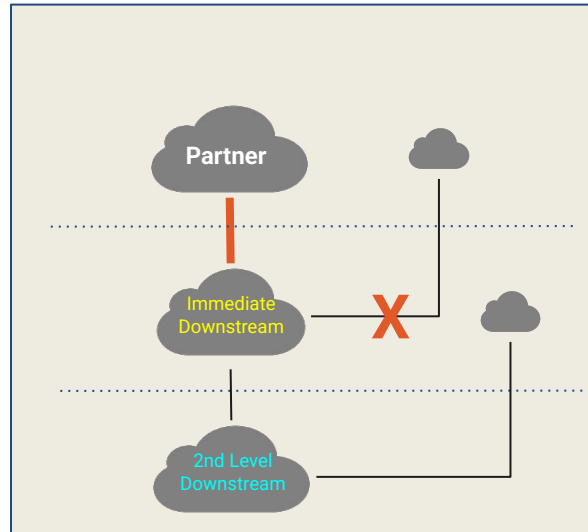
Protection for You and Your Customers

Infrastructure Protection



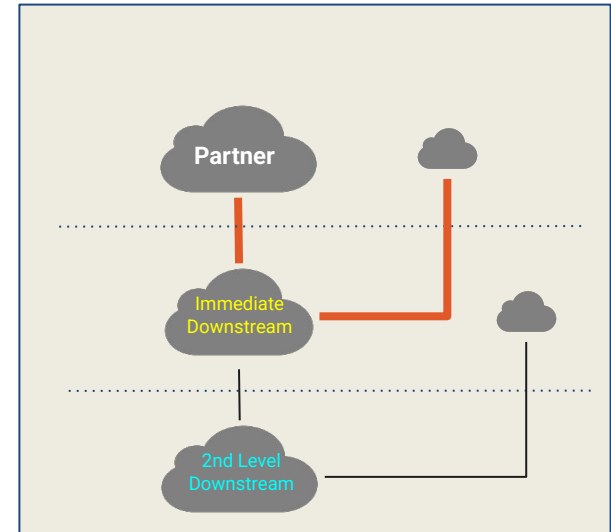
Protecting prefixes assigned to partner's infrastructure.

Clean Pipe (CP)



Ensuring the pipe connecting to downstream is attack free.

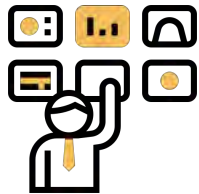
Total Protection (OP & AP & DP)



Preventing attacks hitting downstream customers from any of their IP transit links.

A Cloud Platform Built into a Box

24/7 Platform Monitoring



Nexusguard will monitor the platform health, utilization and status 24x7.

Software Upgrade & Maintenance



Constant software upgrades, new features, detection and mitigation signatures and tools

Market Place



Growing library of NXG and 3rd party applications, e.g. integration with technology vendors such as fortinet, AWS, and other providers, which can be sold as VAS.

Essential features in attack handling



AI Driven DDoS
detection &
mitigation



Multi-tenancy
portal



WAF protection



Cloud Offload



Remote DDoS
monitoring



Attack alert



TLS protection



Managed SOC



Auto traffic
diversion



Report



Load balancing



Auto traffic
baselining



FlowSpec





CSP Solutions Overview



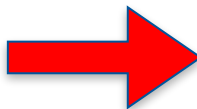
Telco as Customer



Telco as Partner
\$\$\$

Telco internal Consumed Services Core Infrastructure Protection

	Mitigation	Detection	End user Customization
Infra Protect	YES	-	-
NXG Origin Protection For CSP	YES	YES	YES
TAP Program	YES	YES	YES
Business Model			



TAP Partner Delivered Solution End user protection plus Upsell Opportunities

Local Clean Pipe	Local Clean Pipe w/ Global offload	Origin Protection	Application Protection (WAF)	DNS Protection
YES	YES	YES	YES	YES
Cost price to be provided				

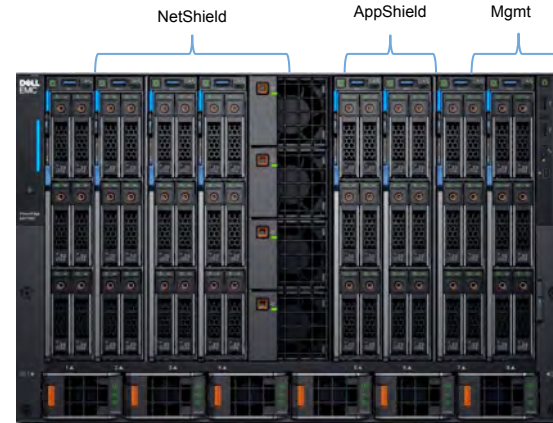
NEXUSGUARD[®]

TAP Program



TAP Managed DDoS Fees	
License	Netshield and Management Software License for up to 40Gbps/100Gbps/200Gbps DDoS Scrubbing
	AppShield Software License to serve up to 160,000 req/s. For Web Proxy, WAF, Load Balancing, Gateway Services.
	Remote Flow Analysis - 10K Flow per second
	Flow Log Retention - 1TB
Maintenance	Technical Support for Nexusguard Hybrid Instance - 24x7 Hybrid - On-premise Systems + Partner Cloud Instance
	Software maintenance and upgrades Software and Systems Debugging and Troubleshooting Software and Systems Support
Managed Support	Nexusguard Tier 2 SOC Support - 24x7, Refer to Support Level Document
	Nexusguard Tier 3 SOC Support - 24x7, Refer to Support Level Document
	Nexusguard Tier 4 SOC Support - 24x7, Refer to Support Level Document
Enablement & Training	Enablement pack
	Module 3 - Sales Training,
	Module 4 - Pre-Sales Training,
	Module 5 - Product Training,
	Module 6 - Marketing Support
	Online Training and Webinars
	2 x Certified Security Analyst (Level 1 SOC Support) - Yearly Recertification, per head
	Access to all related go-to-market collaterals including Brochures, Datasheets, FAQ, Battlecards, etc
Access to all research related content - DDoS Reports, Threat Intelligence resources, Blog pieces, etc	
Access to all marketing campaign related content - EDM Pack, Press Releases, etc	

Nexusguard Cloud-in-a-box Mx7000



Managed DDoS Support Fees component :



Category	Details
	TAP Managed DDoS Fees includes :
License and set up fees	1 year Netshield and Management Software License for up to 200Gbps DDoS Scrubbing. 50K Flow Per Second Flow Monitoring. Max 5 Routers 1 Year AppShield Software License to serve up to 160,000 req/s. For Web Proxy, WAF, Load Balancing, Gateway Services.
	Project Management Fee - Per Site
	Network Architecture Design & Consultancy
	Hardware Installation & Configuration
	MX7000 mitigation Platform Software and network installation and configuration.
	NXG Cloud Instance Setup and configuration
	Remote Flow Analysis - 90K Flow per second
	Flow Log Retention - 1TB
	POC & UAT
Maintenance	Monitoring of Hybrid Servers installed at Partners location. Monitors system metrics such as CPU Usage, Memory Usage, Harddisk Capacity, Disk I/O, etc. Per Site
	Monitoring of Components and Service installed at Hybrid Servers. Monitors daemons, processes, and services.
	Technical Support for Nexusguard Hybrid Instance - 24x7 Hybrid - On-premise Systems + Partner Cloud Instance
	Software maintenance and upgrades
	Software and Systems Debugging and Troubleshooting
	Software and Systems Support



Managed DDoS Support Fees component :



Category	Details
Managed Support	Nexusguard Tier 2 SOC Support - 24x7, Refer to Support Level Document
	Nexusguard Tier 3 SOC Support - 24x7, Refer to Support Level Document
	Nexusguard Tier 4 SOC Support - 24x7, Refer to Support Level Document
Enablement & Training	<p>Enablement pack</p> <p>Module 3 - Sales Training,</p> <p>Module 4 - Pre-Sales Training,</p> <p>Module 5 - Product Training,</p> <p>Module 6 - Marketing Support</p> <p>Online Training and Webinars</p>
	2 x Certified Security Analyst (Level 1 SOC Support) - Yearly Re-certification, per head
	Access to all related go-to-market collaterals including Brochures, Datasheets, FAQ, Battlecards, etc
	Access to all research related content - DDoS Reports, Threat Intelligence resources, Blog pieces, etc
	Access to all marketing campaign related content - EDM Pack, Press Releases, etc
	Optional add on
Optional	<p>Cloud-Based DDoS Protection for huge attacks</p> <p>Nexusguard InfraProtect - DDoS Management Platform in the Cloud</p> <p>InfraProtect offers CSPs the ability to leverage Nexusguard's globally distributed infrastructure to be used as a off-site sandbox to perform traffic analysis, shaping and DDoS mitigation so that traffic that reaches CSPs' network are always clean.</p> <ul style="list-style-type: none"> - Access to 2.24Tbps, 1 Billion PPS capacity - Unlimited Attack Protection Coverage



Operation Tier Definition



Tier-4

Troubleshooting Assistance

Feature Development

Platform Hotfix

Platform Upgrade

Platform Delivery

Service/Case Review

Tier-3

Maintenance Notification

Service Recovery

Log Analysis

POC Support

Attack Mitigation

Incident Summary & Report

Tier-3 Troubleshooting

Feature Request

Bug Report

Tier 4 Escalation

Tier-2

Platform Monitoring

POC Support

Attack Handling

Service Recovery

Tier-2 Troubleshooting

Request Fulfillment

Tier 3 Escalation

Tier-1

Client Coordination

Data Gathering

Monitoring

Initial Troubleshooting

Tier 2 Escalation

**Service Desk +
Event Management**

Incident Management

Request Fulfillment

**Problem Management +
Platform Management**

Escalation

Nexusguard Partner Eco-systems



What we have to offer our partners?

People

- Training & Certification
- Global Network of shared experience
- Self-service knowledge base

Process

- Cyber Defense & Mitigation Methodology
- Monitoring, Evaluation & Analytics, and Response Process
- Operations Support

Technology Framework

- DDoS Mitigation
- Global Offload
- Seamless Integration
- Easy Access Sales & Marketing Portals



Referral

Get referral \$s and build up your partner points



Reseller

Easily bundled solutions into your products/services



Cloud Reseller

Enhanced Customer Intimacy
Co-branded Portal



TAP

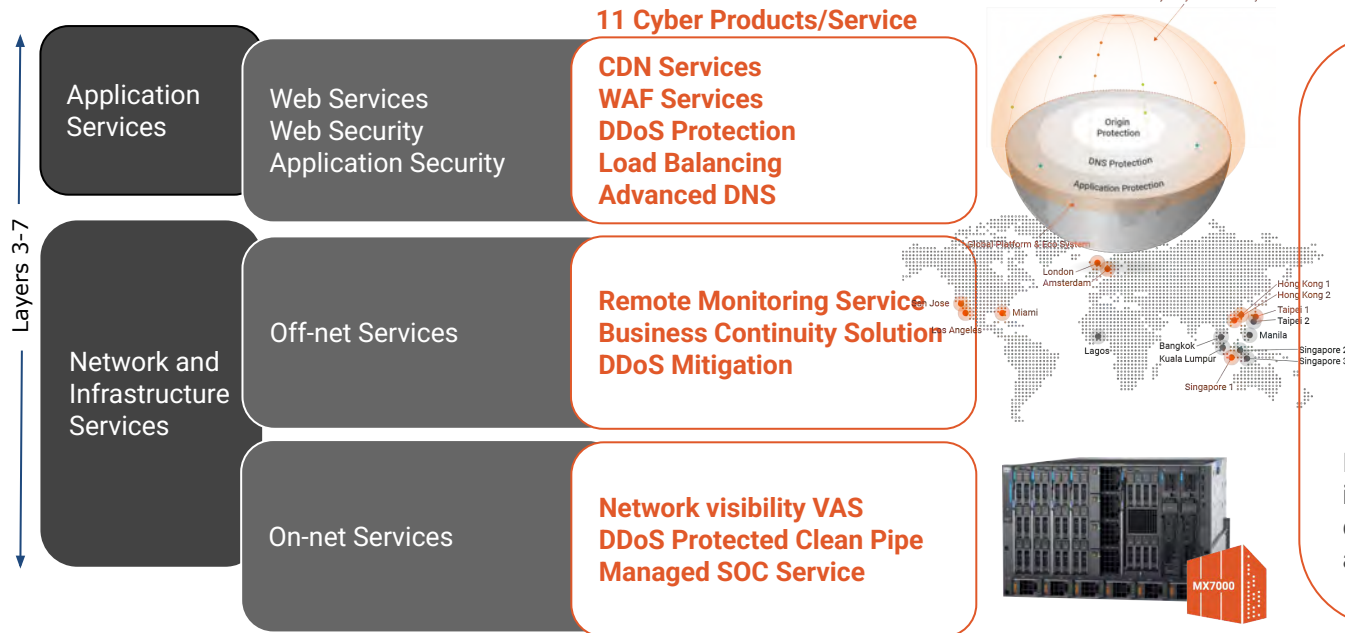
Deep Bundled Differentiation
Fast GTM
Differentiated Offering,

Hybrid

NEXUSGUARD[®]

The True Value of TAP -

Rejuvenate old pipelines. Open new markets.



True Hybrid DDoS Protection for CSP clients

- On-premise deployment
- Global Cloud Offload
- People, Process & Technology
- Co-label (Your Brand)
- Multi-tenant portal

From design, planning, implementation to training, certification, ongoing maintenance and support.

Table of New Services

OSI Layer	Service	Matching Telco Service	Customer Segment
Network Layer	Clean Pipe	DIA	Downstream ISP, Large Corporate, Universities, Government (MFA, etc) Gaming
	Origin Protection	IP Transit / Multi home	Tier 2 ISP, Data Center hosting, Gaming etc
Application Layer	Application Protection	Hosting customer	Education, FSI, E-Commerce, Large Conglomerate, Gaming
	DNS Protection		Education, FSI, E-Commerce, Large Conglomerate, Gaming

DDoS requirements and solutions by industry sector



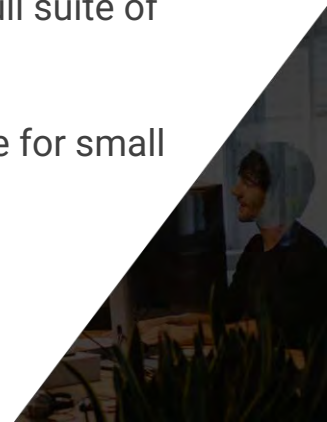
Industry Sector	DDoS Protection Requirements	Solution
Public Sector	Data sovereignty requiring scrubbing within country	Local scrubbing, backed by NXG global offload
	Service management for different government bureaus	Multi-tenant portal
Banking	Compliance and Data sovereignty	Application DDoS protection
Gaming	Performance and Effective protection	Application or Network protection
Downstream ISPs	Preventing link congestion	Local scrubbing, backed by NXG global offload
DataCenter	DDoS free internet links Application Protection (Web/DNS)	Local scrubbing, backed by NXG global offload

Introduction to Bastions



Bastions servers

- 2 models: Bastions DELL **MX7000** & **R660**
- Installed with Nexusguard software & technology for DDoS protection
- MX7000 - HA model suitable for large CSPs & mega PoPs requiring a full suite of services
- R660 - standalone model suitable for small CSPs or satellite PoPs





NEXUSGUARD®

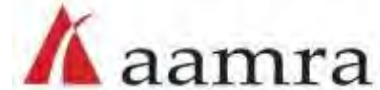
DDoS Protection Made Simple

Successes

Some Of Our Customers



Some of Our Customers



Govt - \$50m deal to keep Govt website going in a cyberattack

- Federated portal enables cybersecurity service management at national, bureau and department levels
- Comprehensive protection for web and DNS.



Dr Chong Yoke Sin, chief of StarHub's enterprise business group, said it will provide the Singapore Government with its telco-centric security operations as well as the cloud-based mitigation services of its technology partner Nexusguard.

<http://www.straitstimes.com/tech/50m-deal-to-keep-govt-websites-going-in-a-cyber-attack>

Value propositions of Nexusguard services

- Proven Success Formula
- Partnership Model
- Increase Revenue/Reduce Churn
- Lower Total Cost of Ownership
- Brand Value
- Speed to Market
- Training/Certification
- SLA



A solid orange vertical bar positioned to the left of the main title.

Multi Tenancy Portal

Admin and Customer portal

Admin Portal

The screenshot shows the NexusGuard Admin Portal interface. The browser address bar displays `nexusguard.com/main.html#/customer_list`. The page title is **NEXUSGUARD**. The navigation menu includes Dashboard, Customer, Activity, Resources, and Apps. The main content area is titled "Customer List" and contains a table with the following columns: ID, Customer ID, and Service. The table lists various customer entries with their respective service details. Annotations with red arrows point to the "Partner's url" in the browser bar, the "Partner's logo" in the top left, and a specific customer entry in the table labeled "Partner's customer".

ID	Customer ID	Service
1449	SPS-485655-SOC_TEST	Application Protection, DDoS Protection, DNS Protection, CDN Protection, Clean File
1448	SPS-438629-DDNS_LIVE	DNS Protection
1445	SPS-427947-golaxyBackup	Application Protection, DDoS Protection, DNS Protection, CDN Protection, Clean File
1429	SPS-411335-4405PH4E_MBT	Application Protection, DDoS Protection, DNS Protection, CDN Protection, Clean File
1428	SPS-382761-HAUSTEWAFF	Application Protection, DDoS Protection, DNS Protection, CDN Protection, Clean File
1422	SPS-441532-8403kites	Application Protection, DDoS Protection, DNS Protection, CDN Protection, Clean File
1369	SPS-420019-40Net	Application Protection, DDoS Protection, DNS Protection, CDN Protection, Clean File
1341	SPS-425829-8684PivotalDesk	DDoS Protection
1259	SPS-417326-56DZ	Application Protection, DDoS Protection, DNS Protection
1173	SPS-425829-84403kites	DDoS Protection
1172	SPS-488021-1PKK_TH_POC	DDoS Protection
1014	SPS-620261-LAC_TEST	Application Protection, DDoS Protection, DNS Protection
1006	SPS-482769-Ap4Power_POC	Application Protection
991	SPS-521849-Capitaland_POC	Application Protection
988	SPS-422268-8684PivotalDesk	Application Protection

Customer Portal

The screenshot shows the NexusGuard Customer Portal interface. The top navigation bar includes Overview, DDoS Alert, and Traffic. The Overview section displays three key metrics: 41.6, 20.1, and 25.1. The Traffic section shows a line graph of traffic over time, with a legend for Traffic In and Traffic Out. The Active Mitigation section displays a bar chart showing the number of active mitigations, with a legend for Bot and Clean. The overall layout is clean and modern, with a focus on real-time monitoring and alerting.

Multi-tenancy portal simplify your client management, you can provision, monitor, mitigate attack in a single location

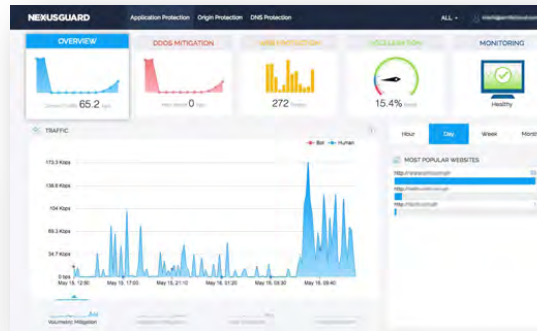
Each customer will have their own portal to view the DDoS protection service they purchase from you.

Customer Portal

AP - WAF



AP/OP - Normal Traffic



AP - Cache



AP/OP - DDoS Attack Event



AP - Monitoring



<https://support.nexusguard.com/>

NEXUSGUARD®

Automatic Monthly Statement



Dashboard → Report



- Bandwidth Usage
 - Clear and Raw
- Monthly Traffic Analytics
 - Volumetric & Application Mitigation
 - Most Popular Domains
 - Visitor Map, Browsers, Mobile Visitors, Active Pages, Monthly Events
- DDoS Events
 - Largest Attack
- WAF Events
 - Largest WAF Event
 - Top Threat Country
 - Top Targeted URL

NEXUSGUARD™

ACADEMY

Nexusguard Academy was established to offer cybersecurity courses to help enable CSP to become cyber security managed providers and individuals to be practitioners trained by our practitioners.

The courses were designed by Nexusguard practitioners who have years of experience in understanding the gaps of organizations, resolving these gaps by creating applied knowledge transfer from our practitioners to your practitioner so that you can mitigate and remediate cyber attacks.



Partner Ecosystems



What we have to offer our partners?

People

- Training & Certification
- Global Network of shared experience
- Self-service knowledge base

Process

- Cyber Defense & Mitigation Methodology
- Monitoring, Evaluation & Analytics, and Response Process
- Operations Support

Technology Framework

- DDoS Mitigation
- Global Offload
- Seamless Integration
- Easy Access Sales & Marketing Portals



Referral

Get referral \$s and build up your partner points



Reseller

Easily bundled solutions into your products/services



Cloud Reseller

Enhanced Customer Intimacy
Co-branded Portal



TAP

Deep Bundled Differentiation
Fast GTM
Differentiated Offering,

Hybrid

NEXUSGUARD®

NEXUSGUARD®

AFR-IX
telecom

Commercial Benefits

Commercial Benefit - Gaining Marketing Share



1) Cleanpipe

- a) Helps Telco to **INCREASE REVENUE** (eg. top up protection when selling a new / existing connectivity)
- b) Helps Telco to **MAINTAIN REVENUE** (eg. include protection into connectivity contract in the event facing competition. Therefore reduce the possibility of total loss of revenue)
- c) **Disrupt the market** - ISP able to sell a premium connectivity service as they can easily include protection in their service and charge at a slightly higher premium

2) Origin Protection

- a) Helps Telco to **INCREASE REVENUE** by selling protection to multi home customers (this will position Telco as a One Stop Shop center for their cyber security services)
- b) Helps Telco to **GAIN REVENUE** and new customers as this protection is able to protect "offnet" customers as well

3) Application Protection

- a) Helps Telco to increase revenue by approaching existing customers to upgrade their protection plans to cover protection for their website and applications

Commercial Benefit - Renewal Customers

ISP prices have been under heavy downward pricing pressure for a number of years. Meanwhile DDoS attacks have consistently been on the upward trend. Today, DDoS attacks have become mainstream.

With the new service, Telcos can choose one of 2 strategies.

- 1. Offer DDoS protection as a value add and maintain prices**
- 2. Offer DDoS protection into the DIA package and increase prices by X%.**

- Cloud vs. bastions
- Bastions use cases
- Program comparison



Appendix

Introduction to Nexusguard services

Nexusguard Cloud services

- offered solely by Nexusguard
- suitable for most deployment scenarios
- provide always-on / on-demand protection to web / server / network
- distributed scrubbing centres are fully owned & operated by Nexusguard
- offer AP/DP/OP services to any client - “sell to” service

+

Nexusguard Bastions

- jointly offered by Nexusguard & partner
- suitable for on-premise / hybrid deployments
- scrubbing platform is jointly operated by Nexusguard & partner
- offer AP/CP/DP/OP services to partner’s clients - “sell through” service

True Hybrid vs. Other Solutions

Benefits	Blackhole	Traditional Clean Pipe	On-Premise	Cloud Based	On-demand Hybrid	True Hybrid
Volumetric Protection	X	limited	limited	unlimited	unlimited	unlimited
Application Protection	X	X	✓	✓	✓	✓
Collateral Damage Control	✓	✓	✓	✓	✓	✓
Time to Mitigate	seconds	1-3 mins	1-3 mins	3-15 mins	1-15 mins	1-3 mins
Network Latency	X	unchanged	unchanged	higher	higher in cloud	local unchanged
Service Portal	X	X	Local only	Cloud only	Seperated	Integrated
Data Integration	n/a	n/a	n/a	n/a	X	✓

A solid orange vertical bar positioned to the left of the main title.

Comparison analysis

Comparison between appliance, Platform as A Service and Cloud

Eg of vendor		Nexusguard	Arbor, F5, A10, Fortinet, Radware	Cloudflare, Akamai, Imperva
Category	Details	PAAS	Appliance	Cloud
Amortised cost	Subscription based. Eliminate huge upfront investment	Yes	No	Yes
Unlimited product lifespan	Product will eliminate the risk of product EOL. Traditional hardware lifespan usually will be around 5 years which then will require to be refresh once reaches the hardware maturity. Hence tech refresh will incur another round of huge investment	Yes	No	Yes
Skill required to support	Resources required to support product	Minimum	High	Minimum
Productize service	Productise the protection and convert it into a service that end client can subscribe	Yes	Yes	No
Reselling	Able to resell vendor service to protect their customer	Yes with Nxd Cloud service	No	Yes
Co-branding	Able to create own branded service to position in market	Yes with NXG co-branded portal features	Yes, but will need human resources and additional technology to support the services	No
Data Sovereignty Policy	Able to comply to in country data sovereignty requirement	Yes with Nxd Cloud in box implementation in partner network	Yes	No if the cloud POP is not located at the required region

Comparison between DDoS technology implementation

Eg of vendor	Upstream provider	Upstream provider	Arbor, Radware, F5	Cloudflare, Akamai, Imperva	Arbor+Arbor Cloud, F5+Silverline, FortiDdos+Nexusguard	Nexusguard
DDoS Implementation method	Blackhole	Clean Pipe	On-Premise	Cloud Based	On-demand Hybrid	True Hybrid
Volumetric Protection	x	limited	limited	unlimited	unlimited	unlimited
Application Protection	x	x	x / ✓	✓	✓	✓
Collateral Damage Control	✓	✓	✓	✓	✓	✓
Time to Mitigate	seconds	1-3 mins	1-3 mins	3-15 mins	1-15 mins	1-3 mins
Network Latency	x	unchanged	unchanged	higher	higher in cloud	local unchanged
Service Portal	x	x	✓	✓	✓	✓ (up to host based)
Data Integration	n/a	n/a	n/a	n/a	x	✓
Zero Day Attack	n/a	n/a	n/a	n/a	x	✓

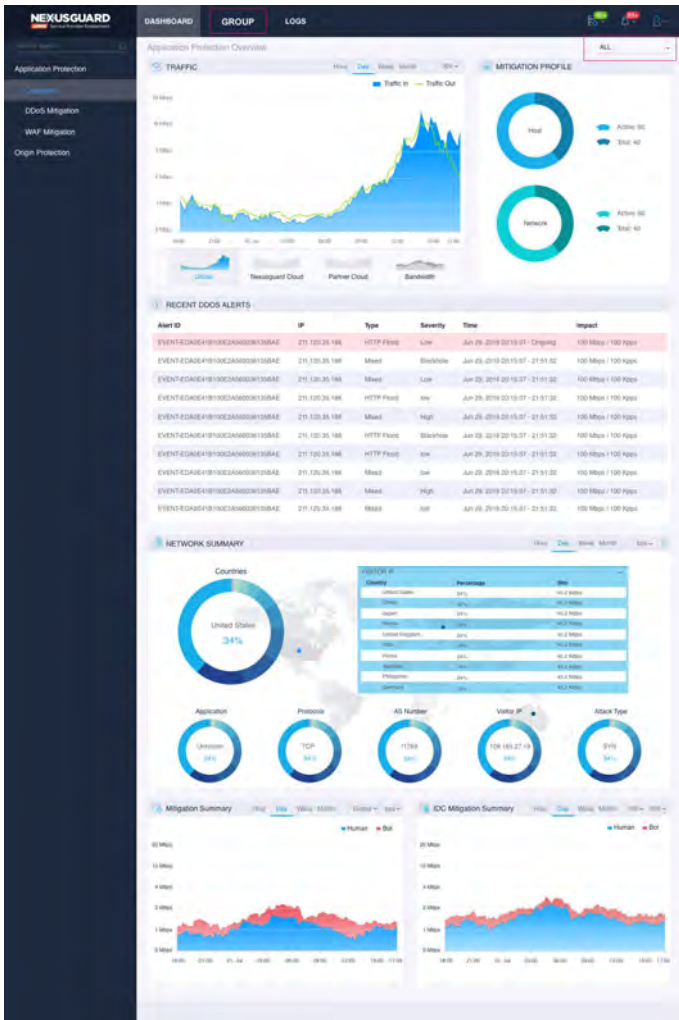
A solid orange square is positioned to the left of the text.

Thank you !

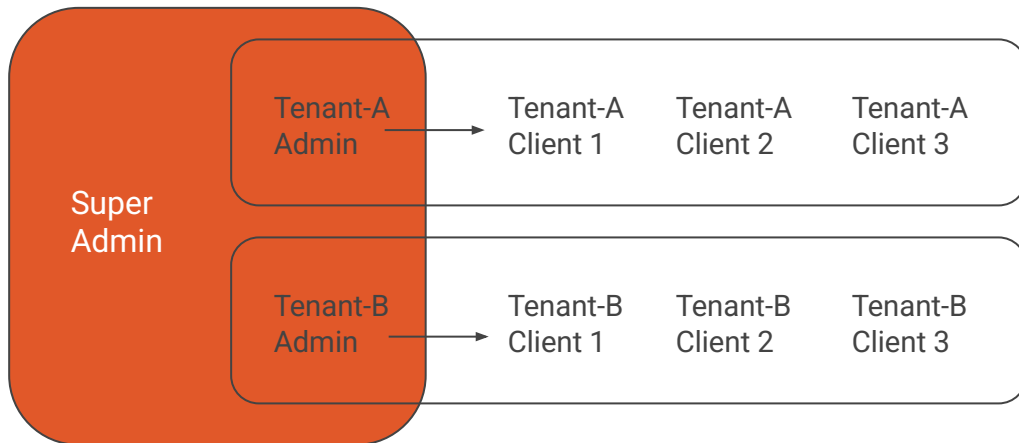
A solid orange vertical bar positioned to the left of the section header.

APPENDIX

Case Studies



Super Admin Dashboard



Super Admin Tenant Management

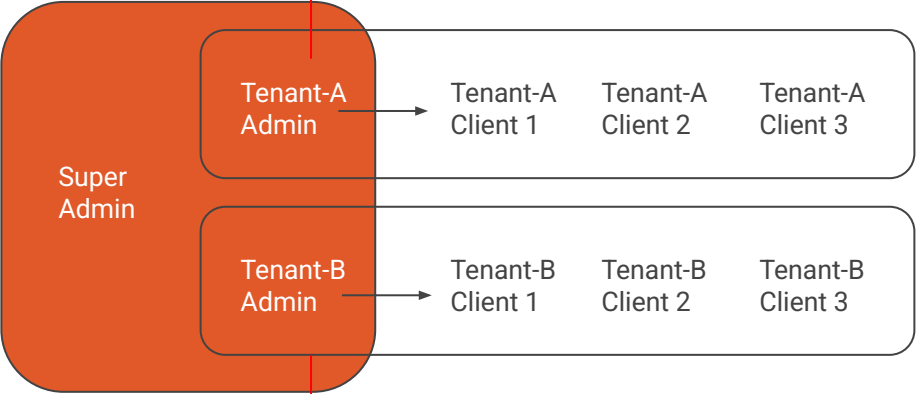


Navigation: DASHBOARD | **GROUP** | LOGS

Partner List

ID	Group	Customer
0001	SPE-YXG	58
0002	SPE-YIN	159
0003	SPE-ACE	97
0004	SPE-MSG	115
0005	SPE-SEW	83
0006	SPE-HNY	13
0007	SPE-DEM	25
0008	SPE-UDK	76
0009	SPE-YIN	218
0010	SPE-SEW	102
0011	SPE-HNY	134

Page 1 of 3



Super Admin Tenant-Client Management



DASHBOARD

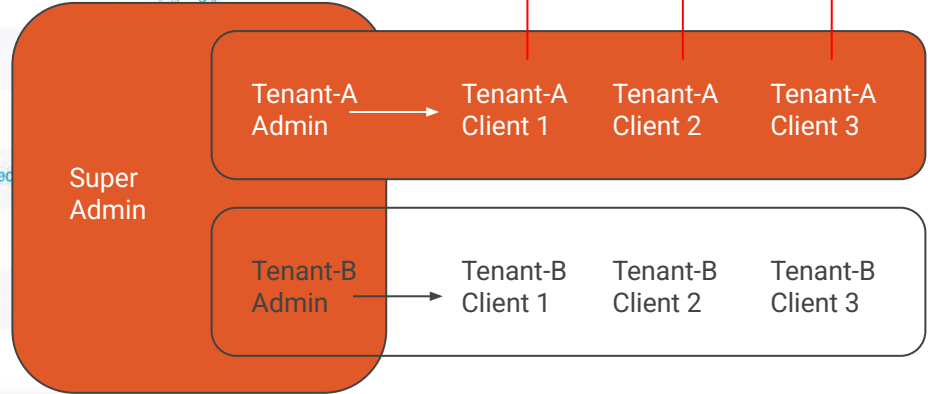
GROUP

LOGS



Partner List > SPE-HNY Customer List

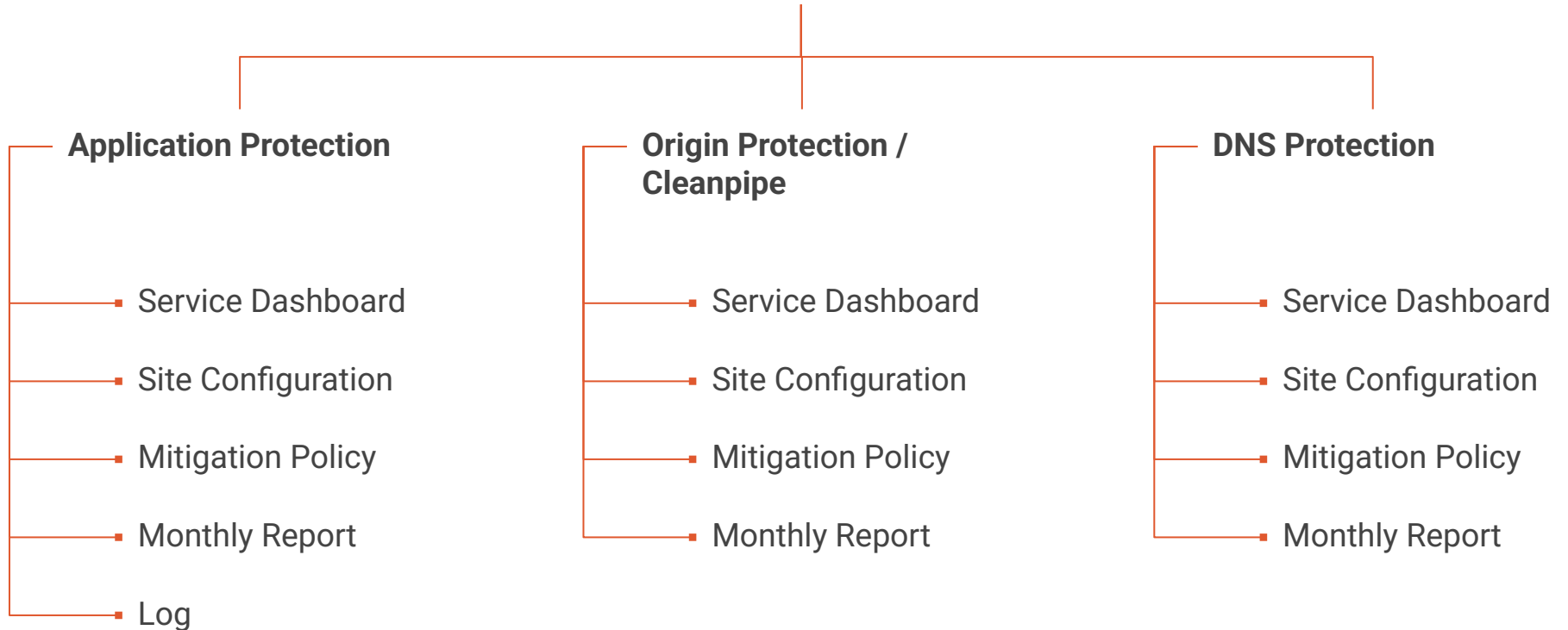
ID	Customer	Service	Settings
0001	NXG-609856-YXG	Application Protection DNS Protection	
0002	NXG-718719-YIN	Origin Protection	
0003	NXG-418552-ACE	DNS Protection	
0004	NXG-683370-MSG	Application Protection Origin Protection DNS Protection	
0005	NXG-723372-SEW	Origin Protection DNS Protection	
0006	NXG-366208-HNY	Application Protection	
0007	NXG-519380-DEM	Application Protection	
0008	NXG-408336-UDK	Origin Protection	
0009	NXG-918871-YIN	DNS Protection	
0010	NXG-902561-SEW	Application Protection	
0011	NXG-401328-HNY	DNS Protection	



Customer Portal Structure

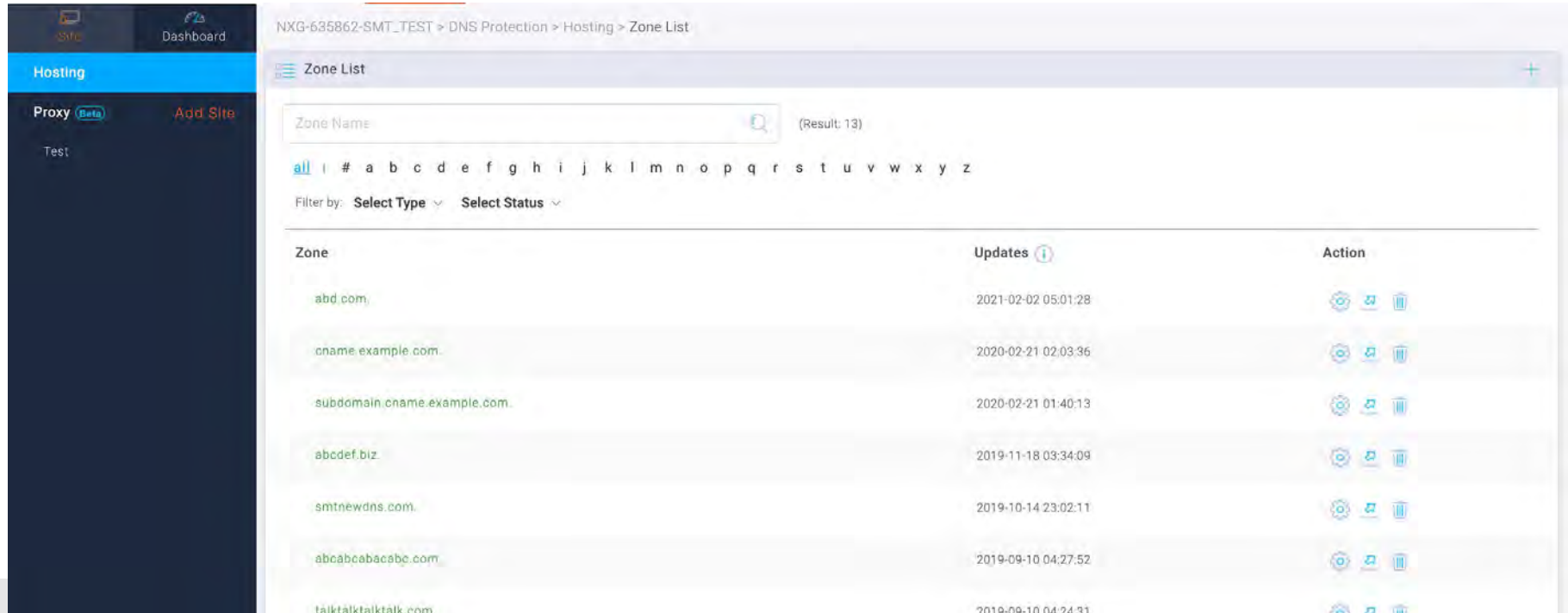


Customer Portal

























DNS Protection

- Federated portal enables cybersecurity service management at national, bureau and department levels
- **Comprehensive protection for web and DNS.**



The screenshot displays a web management interface for DNS Protection. The breadcrumb navigation shows the path: `NXG-635862-SMT_TEST > DNS Protection > Hosting > Zone List`. The main content area is titled "Zone List" and includes a search bar for "Zone Name" with a magnifying glass icon and a "(Result: 13)" indicator. Below the search bar is a keyboard layout for filtering, with "all" selected. There are also "Filter by: Select Type" and "Select Status" dropdown menus. The main table lists DNS zones with columns for "Zone", "Updates" (with an info icon), and "Action" (with icons for settings, refresh, and delete).

Zone	Updates (i)	Action
<code>abd.com.</code>	2021-02-02 05:01:28	  
<code>cname.example.com.</code>	2020-02-21 02:03:36	  
<code>subdomain.cname.example.com.</code>	2020-02-21 01:40:13	  
<code>abcdef.biz.</code>	2019-11-18 03:34:09	  
<code>smtnewdns.com.</code>	2019-10-14 23:02:11	  
<code>abcabcabcabc.com.</code>	2019-09-10 04:27:52	  
<code>talktalktalk.com.</code>	2019-09-10 04:24:31	  

A solid orange vertical bar positioned to the left of the section header.

Case Study 2

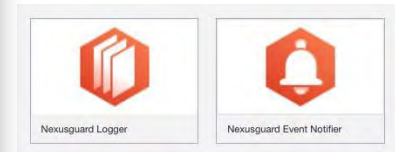
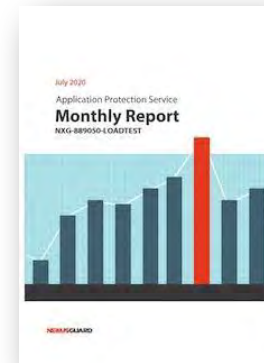
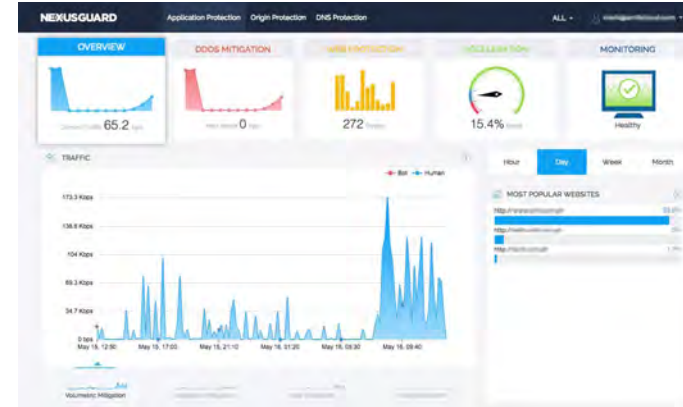
FSI

FSI - Bank Application Protection Requirement




- 27001 & PCI-DSS
- Flexible deployment for L3/4 and L7 protection
- Individual profiling for each website
- Download log and monthly reports

Site/Domain	Smart Route	NetShield	SSL Cipher	AppShield	Cache	WAF	Load Balance
27.11.██████████	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
stark-public-██████████-80	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
stark-public-██████████-443	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27.11.██████████	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
insurance-public-██████████-80	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
public-██████████-80	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
public-██████████-80	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
www-public-██████████-80	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
www-public-██████████-80	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27.11.██████████	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
stark-uk-public-██████████-80	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
stark-uk-public-██████████-443	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27.11.██████████	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
stark-public-██████████-80	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
stark-public-██████████-443	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27.11.██████████	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
stark-public-██████████-80	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
stark-public-██████████-443	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



NEXUSGUARD®

A solid orange vertical bar positioned to the left of the section header.

Case Study 3

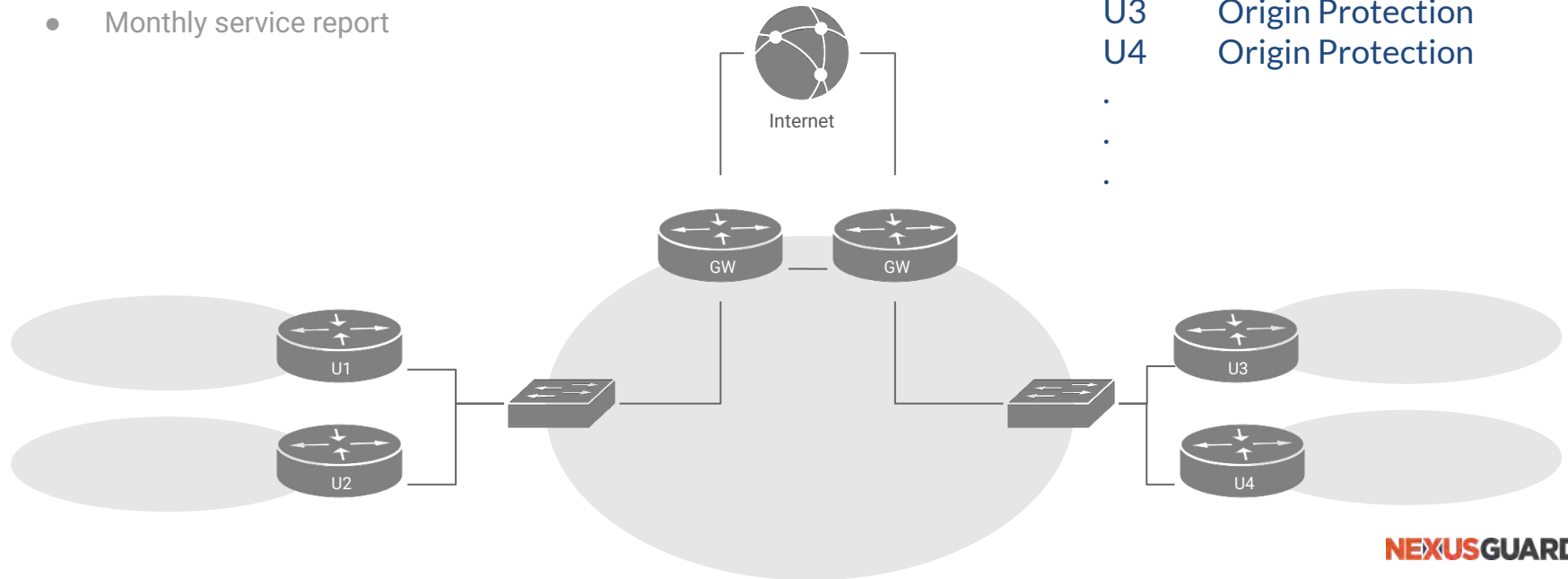
Universities

Academic Network

- **Volumetric protection for all universities**
- **Independent service portal**
- Application & DNS protection at each university's own discretion
- Monthly service report

Customer List

- U1 Origin Protection
- U2 Origin Protection
- U3 Origin Protection
- U4 Origin Protection
-
-
-

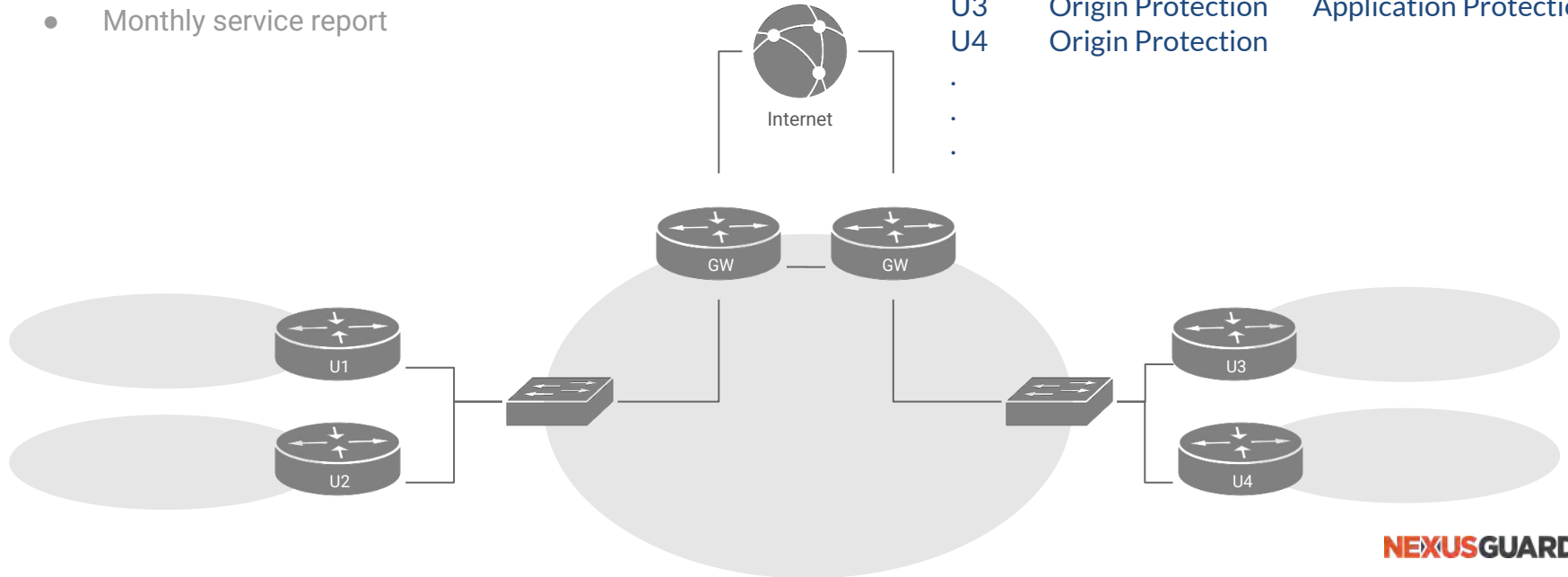


Academic Network

- Volumetric protection for all universities
- Independent service portal
- **Application & DNS protection at each university's own discretion**
- Monthly service report

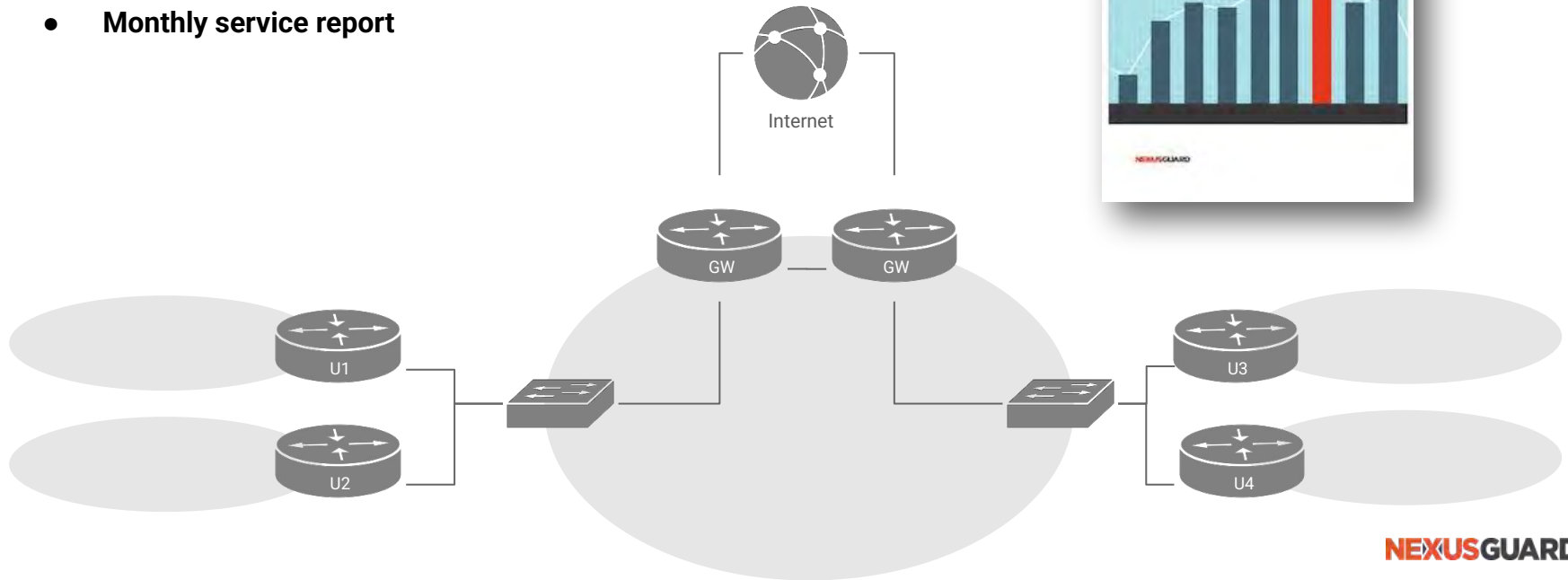
Customer List


U1	Origin Protection	
U2	Origin Protection	DNS Protection
U3	Origin Protection	Application Protection
U4	Origin Protection	
•		
•		
•		



Academic Network

- Volumetric protection for all universities
- Independent service portal
- Application & DNS protection at each university's own discretion
- **Monthly service report**



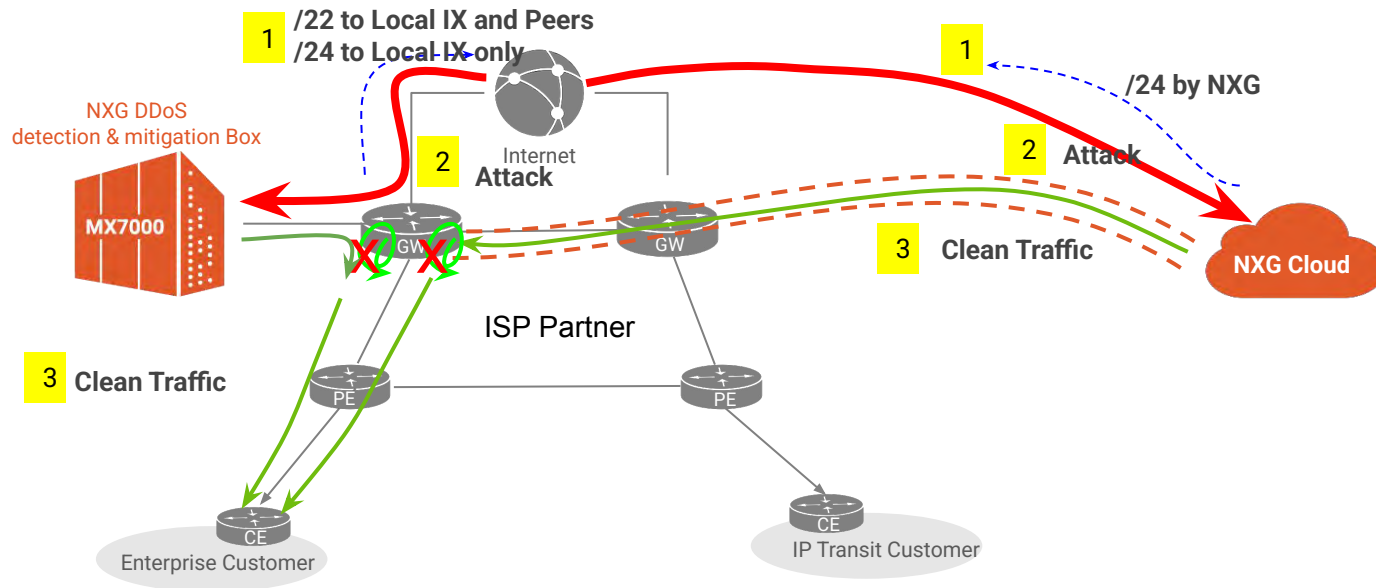
A solid orange vertical bar positioned to the left of the section header.

Case Study 4

Data Center/ISP

Partner Network Infrastructure and Downstream Customer Protection

- **Unlimited attack coverage by global offload**
- None-threshold based for ISP/telco
- Bits and Pieces Attack
- Auto Cloud diversion

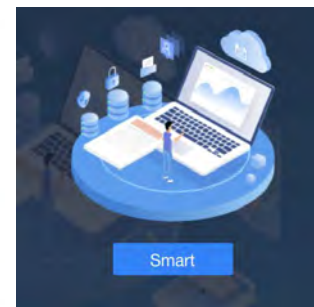
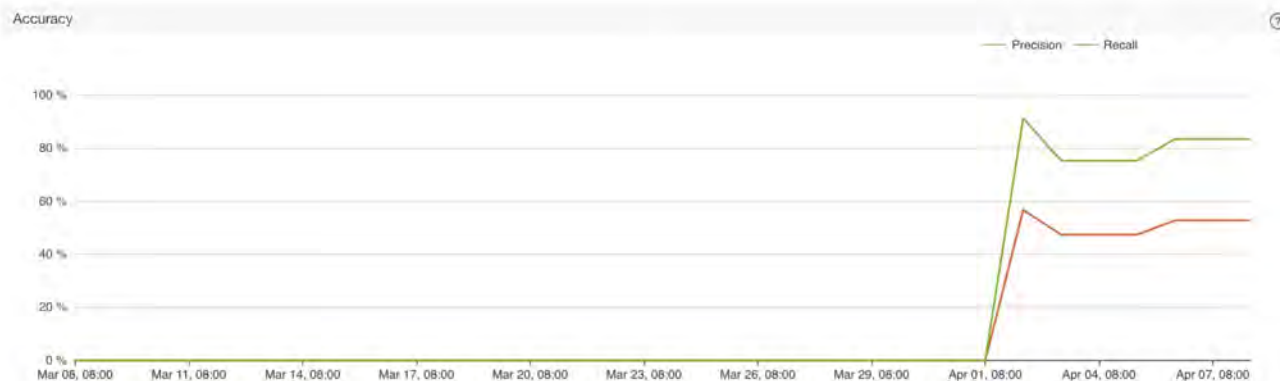


Requirement: Local announcement can be contained within IX

Partner Network Infrastructure and Downstream Customer Protection



- Unlimited attack coverage by global offload
- **None-threshold based for ISP/telco**
- Bits and Pieces Attack
- Auto Cloud diversion



- **Built on Big Data Analysis and Machine Learning**
- **Continuous data modelling to learn change in traffic profile**
- **Get smarter over time and with supervised learning.**
- **No static threshold configuration is needed except for traffic level to activate blackholing**
- **Good at detecting dynamic traffic profiles - seasonal / time of day / natural growth**
- **Learning time shall be allowed**

Partner Network Infrastructure and Downstream Customer Protection



- Unlimited attack coverage by global offload
- None-threshold based for ISP/telco
- **Bits and Pieces Attack**
- Auto Cloud diversion

Network Detection Policy is deployed in normal mode to detect anomalous traffic which exceeds pre-defined detection thresholds for a certain time window, aka. LSP (latency start period, usually about 120 seconds) for an entire /24 network. You can customize the lowest and the highest threshold volume for specific types of attacks.

TCP	Low	High	Direction	Settings
TCP SYN	10 Kpps	100 Kpps	Incoming	<input checked="" type="checkbox"/>
TCP ACK	200 Kpps	300 Kpps	Incoming	<input checked="" type="checkbox"/>

Network Detection (/24)



Partner Network Infrastructure and Downstream Customer Protection



- Unlimited attack coverage by global offload
- None-threshold based for ISP/telco
- Bits and Pieces Attack
- **Auto cloud diversion**



- Minimize actions required by customer
- Shorten traffic diversion lead time
- Reduce operation errors
 - missing attack
 - routing issue



Event ID	Site	Network	Size	Diversion Mode	Start Time	End Time	Option
event-19a4071023386a6f00c02086d3	jwps2_cloud_div1	10.60.8.0/24	9.22 Mbps	Auto Divert	21 Apr 2020 14:35:40	Ongoing	
event-8c13475fb34104a03e113090544	jwps2_cloud_div1	10.60.9.0/24	9.46 Mbps	Auto Divert (Monitor)	21 Apr 2020 14:23:41	Ongoing	
event-ed94957975c61115e1cbac365	jwps2_cloud_div1	10.60.9.0/24	8.84 Mbps	Auto Divert (Monitor)	21 Apr 2020 14:18:41	21 Apr 2020 14:20:41 (2 mins)	
event-ed47b87c1b1c5268964443302	jwps2_cloud_div1	10.60.8.0/24	9.00 Mbps	Auto Divert	21 Apr 2020 10:08:44	21 Apr 2020 11:56:56(1 hrs 48 mins 12 secs)	
event-4a955b713b4e118ba0254d8a0f	jwps2_cloud_div1	10.60.8.0/24	0 tps	Auto Divert	21 Apr 2020 10:08:43	21 Apr 2020 10:11:43(3 mins)	
event-1770e0cd1aa33c52288144b77c	jwps2_cloud_div1	10.60.8.0/24	8.99 Mbps	Auto Divert	21 Apr 2020 09:51:09	21 Apr 2020 10:11:43(20 mins 34 secs)	
event-b146f3a092138e6c1002d6d93	jwps2_cloud_div1	10.60.8.0/24	8.90 Mbps	Auto Divert	20 Apr 2020 18:51:41	20 Apr 2020 19:04:32(12 mins 51 secs)	
event-a25153569450b572cae7724c03	jwps2_cloud_div1	10.60.8.0/24	0 tps	Auto Divert	20 Apr 2020 18:51:40	20 Apr 2020 18:54:39(2 mins 59 secs)	
event-0b234c911d1e3bb5072929b3	jwps2_cloud_div1	10.60.8.0/24	8.90 Mbps	Auto Divert	20 Apr 2020 18:46:57	20 Apr 2020 18:54:39(7 mins 42 secs)	
event-455477a1ca12375300c781833bc	jwps2_cloud_div1	10.60.8.0/24	1.13 Mbps	Auto Divert	20 Apr 2020 16:46:04	20 Apr 2020 18:36:40(1 hrs 50 mins 36 secs)	
event-cfb656bc7e7f6e6638dc2e8d1	jwps2_cloud_div1	10.60.12.0/24	0 tps	Divert	16 Apr 2020 17:52:05	20 Apr 2020 14:40:52(92 hrs 48 mins 47 secs)	

