Monetization of Arbor Networks and Cisco Systems DDoS Protection Solutions

According to a recent study by Infonetics Research, revenue from Managed Security Services will increase a whopping 40% over the next 5 years to $22.2 billion in CY19.

Cloud and CPE Managed Security Services Annual Worldwide and Regional Market Size and Forecasts: 2015

Another study by Frost & Sullivan (Analysis of the Global Distributed Denial of Service (DDoS) Mitigation Market, July 2014) indicates:

"DDoS risk, and consequently, demand for DDoS mitigation is increasing due to:

- Growth in the maximum and average sizes of DDoS attacks
- An increasing frequency of DDoS attacks including more sophisticated DDoS attack techniques
- Attack tools and for-hire services enable a broader range of threat actors
- A new element of data theft and network intrusion associated with DDoS attacks"

Growing Need for DDoS Protection Services

The facts are clear—DDoS attacks continue to rise in size, frequency, and complexity. In response, there has been an increase in demand for DDoS protection services. According to Arbor Networks' 10th Annual ***Worldwide Infrastructure Security Report,*** 70% of Service Providers experienced an increase in demand for DDoS protection services.

Why?

For comprehensive DDoS protection, industry best practices recommend an integrated combination of in-cloud and on-premise DDoS protection. In other words… Enterprises can't do it alone and need the help of their service providers to stop modern day DDoS attacks.

According to a recent study by Infonetics Research *(Cloud and CPE Managed Security Services Annual Worldwide and Regional Market Size and Forecasts: 2015),* revenue from Managed Security Services will increase a whopping 40% over the next 5 years to $22.2B in CY19. The report also states…

> *"Despite the slowly improving global economic picture, the managed security service market (particularly the cloud segment) is strong and growing, driven by (amongst other things) an increase in the volume, variety, and complexity of threats of all types, from infrastructure-level threats like DDoS attacks (which are becoming more complex every day) to extremely targeted attacks using 5+ vectors and adapting techniques based on protection detected".*

Clearly, there is a growing demand for DDoS protection services. This paper will provide guidance to deliver a managed DDoS protection service from a combination of Arbor Networks and Cisco DDoS protection solutions.

Best Practices to Stop Modern DDoS Attacks = Opportunity for Service Providers

Modern day DDoS attacks are a dynamic combination of 1) Volumetric, 2) State Exhaustion and 3) Application layer attacks. Industry best practices recommend, that for comprehensive protection from modern day DDoS attacks, organizations must deploy layered protection that is backed by continuous threat intelligence.

In other words. The best place to stop large flood attacks is upstream in a service provider's network before they overwhelm local internet connectivity or on-premises systems. While the best place to stop stealthy application layer attacks are on the customer premises, closest to where key applications and services reside. Just as importantly, the solution must have intelligent communication between these two layers backed by up-to-date threat intelligence to stop dynamic, multi-vector DDoS attacks.

Cloud Signaling Coalition

Today over 60 Service Providers deliver DDoS protection services based on Arbor's technology. They include:

- Axtel
- Aixit
- Allstream
- Bezeq International
- Bharti Airtel
- CAT Telecom
- Circular/Depulsio
- Colt
- Embratel
- FASTWEB
- Hellenic Telecommunications
- Organization (OTE S.A.)
- Jaguar Network
- NextGen Networks
- Gen-I
- Neo Telecoms
- NexusGuard
- Optus
- OrangePolska
- Starhub
- Swisscom
- Tata Communications
- Telefonica
- TelstraClear
- True Internet Co. Ltd
- Vocus

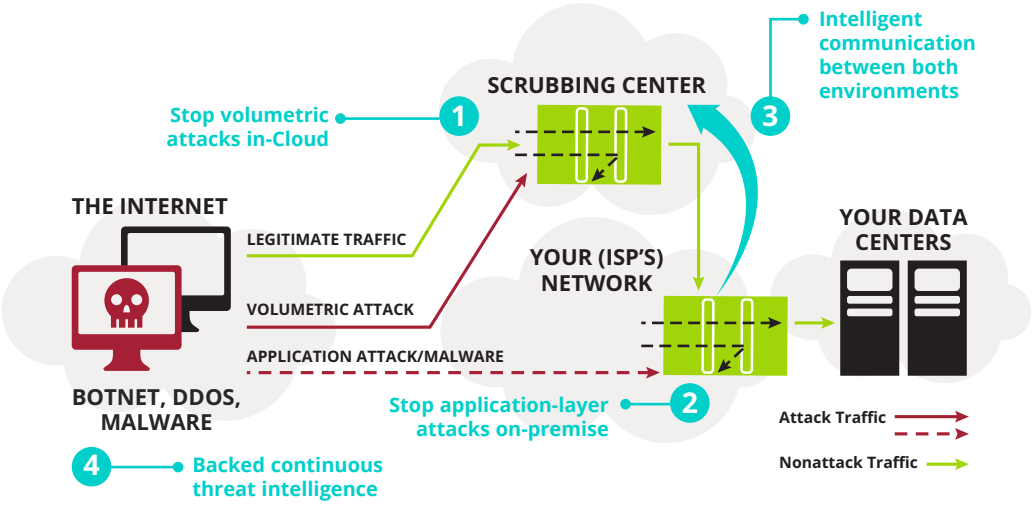

Figure 1: Best practices for comprehensive DDoS protection

Monetization of DDoS Protection Services

As previously noted, Service Providers are well positioned to deliver layered DDoS attack protection solutions. For the past 15 years, Arbor Networks has been the undisputed leader in DDoS attack research, products, and services. In fact, today over 60 Service Providers deliver DDoS protection services based on Arbor's technology. Listed to the left are some of those providers who are also members of Arbor's *Cloud Signaling Coalition.* If fact, Arbor Networks has their own managed DDoS Protection Service called *Arbor Cloud.*

Arbor Networks recently partnered with Cisco, the industry leader in network infrastructure to provide a comprehensive, network embedded, DDoS protection solution. More specifically, Arbor Networks' TMS software, used to surgically mitigate DDoS attacks, can run in the Virtualized Services Module (VSM) of the Cisco ASR 9000 router—collectively known as **Cisco ASR 9000 vDDoS Protection solution.** (For more information visit: *www.arbornetworks.com/asr9000*)

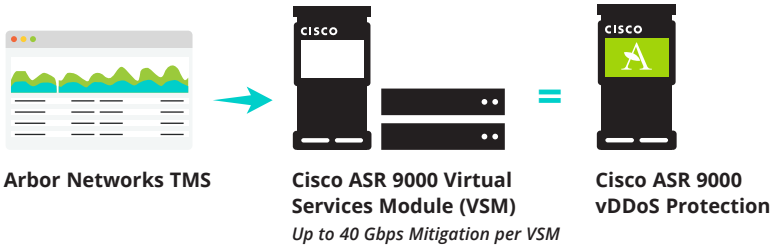

Figure 2: Arbor Networks and Cisco provide comprehensive DDoS protection solution

The following diagram represents a typical deployment of DDoS protection solutions from both Arbor Networks and Cisco. Each of these products can be monetized to deliver managed DDoS protection services.

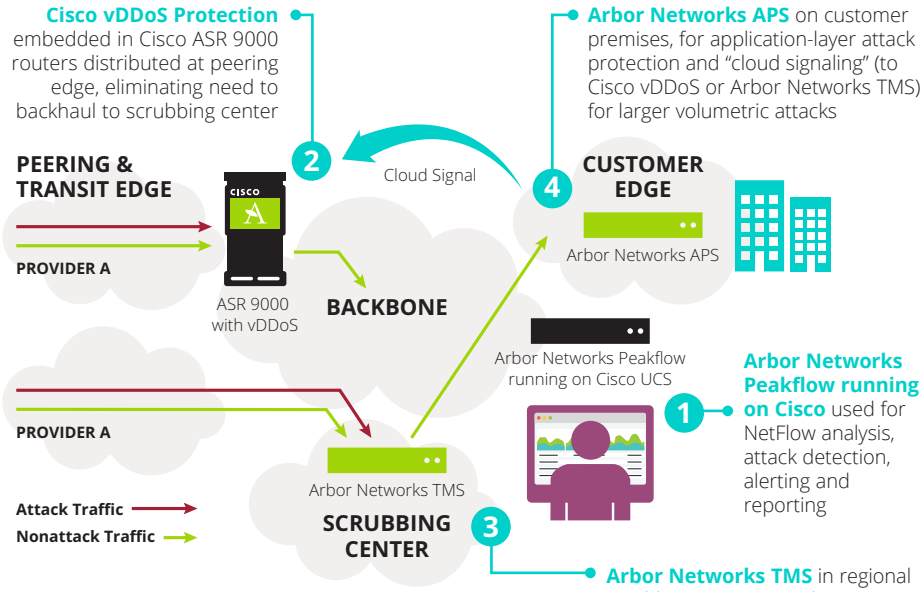

Figure 3: Arbor Networks and Cisco DDoS protection products

Common Components of a DDoS Protection Service

All Managed DDoS Protection Services are different. This is due to the fact that several factors influence the design, packaging and pricing of a managed DDoS protection service. With that said, there are some common components to most DDoS protection services. They are:

- In-cloud vs. on-premise
- On-demand vs. subscription
- Attack detection vs. mitigation
- Access to customer portals & reporting
- SLA, legal terms and conditions of service

The simple table below outlines how these common components are typically used to deliver different DDoS attack protection services. The number of dollar signs ($) denote the relative difference in prices of the services.

FEATURES	Emergency On-Demand	Bronze Subscription	Silver Subscription	Gold Subscription
In-Cloud: On-Demand Mitigation of DDoS attacks	✔			
In-Cloud: Proactive Detection of DDoS, reporting		✔	✔	✔
In-Cloud: Proactive Mitigation of DDoS attacks, reporting and customer portal			✔	✔
CPE-based: Proactive DDoS attack detection, and mitigation				✔
In-Cloud + CPE: Proactive Overflow/Cloud Signaling mitigation of large DDoS attacks				✔
PRICE	**$$$**	**$**	**$$**	**$$$**

All Managed DDoS Protection Services are different. This is due to the fact that several factors influence the design, packaging and pricing of a managed DDoS protection service.

Subscription Services

What is important to note is that these different services are a result of monetizing the different features of the Arbor Networks and/or Cisco DDoS protection solutions. (Refer to Figure 3 for review of Arbor Networks & Cisco DDoS protection products). For example:

- **Bronze Subscription:** In-cloud, pro-active DDoS attack detection service; which can be delivered using Arbor Networks SP software.
- **Silver Subscription:** In-cloud, pro-active DDoS attack detection and mitigation service; which can be delivered using the combination of Arbor Networks SP software (for detection), plus the Cisco vDDoS Protection and/or the Arbor Networks TMS line of products (for mitigation).
- **Gold Subscription:** Combination of in-cloud, pro-active DDoS attack detection and mitigation service; (delivered using the components of the Silver Subscription) plus an on-premises, DDoS attack protection solution that connects to the in-cloud solution during large attacks; delivered using the Arbor Networks APS, Cloud Signaling, in addition to the products mentioned in the Silver Subscription.

Next Steps

Frost & Sullivan Whitepaper
Titled "The Expanding Role of the Service Provider for DDoS Mitigation" explains the unique role MSSPs can play for Enterprise DDoS protection.

Arbor SP & TMS Solution Video
A video describing the key features and benefits of the Arbor DDoS Protection Solution.

Cisco ASR 9000 vDDoS Protection Solutions Video
To learn more about the Cisco ASR 9000 vDDoS Protection Solutions watch this video.

Free DDoS Consultation
For a free DDoS consultation to learn more about how to protect your network and generate DDoS protection service revenue, contact your local Arbor or Cisco representative.

Pricing for DDoS Protection Services

Just as there is no "one size fits" all approach to the design and packaging of DDoS protection services, the same applies to the pricing of these services. Pricing is a decision that is unique to each company. To determine proper pricing for services one must consider several factors such as:

- **Your Target Customers:** Who do you plan on selling these services to and what is their appetite to consume these services? Do you have similar managed security services today? (e.g. managed firewalls or IPS) that you can take queues from? Or will you base the DDoS service as a percent uplift or flat fee based upon existing internet circuits you sell today? (i.e. DDoS protection services can't be 3X the price of internet circuits)
- **Your Competition:** As more and more customers start demanding DDoS protection services, more and more competitors will enter the market. Do you know who your competitors are? Do you know how they price and package their service?
- **Your Company:** Each company has a different set of revenue and profitability requirements. This will have an impact on the price of your service.

Other Best Practices for Delivery of Managed DDoS Protection Services

There is much to consider when designing a Managed DDoS Protection Service. Below are some of the other considerations and best practices.

- **SLAs and Contracts:** Often under estimated components of a DDoS protection service are the Service Level Agreement (SLA) and Service Description contracts. These are critical documents that describe exactly the services your organization will be delivering. They are unique to your service design, level of expertise, size of DDoS mitigation teams, etc.
- **Team and Process:** The best DDoS Protection services in the world have dedicated teams and well documented processes in place. What's more, these processes are constantly tested (e.g. internal War Games) and refined to ensure the teams and service are optimized.
- **Sizing and Over-Subscription:** You need to consider how much capacity will be needed to launch the service initially and what the targeted over-subscription ratio will be for growth planning as your business picks up. A ratio of 10 to 1 is commonly used and may change over time depending upon your scale, the risk your customers have of being attacked, the size of attacks, and the size of your bandwidth to upstream service providers, hosting, web properties, etc.
- **Walk Before You Run:** If you are new to a managed DDoS protection service, it's highly recommend that you start with a limited customer base or geography before you plunge into a full GA service. This allows you to learn, refine your process and also justify the expansion of the service.

Conclusion

We've done this before… call us for further consultation.

Arbor Networks has been exceeding the demands of the most demanding service provider networks globally for over 15 years. These operators trust Arbor Networks to protect their availability and offer the most tested, most reliable, and most trusted DDoS Protection portfolio to protect their customers and make money while doing so. It is no wonder Arbor is called upon to protect the Olympics time and time again. We have helped every type of service provider of all sizes from all parts of the world. We are ready to help you deliver DDoS protection service(s) that are right for your customers and your organization. Call us when you are ready to take the next step and respond to your customer's demands for DDoS protection.