



DDoS Protection for the Network

Greg Smith, Sr. Marketing Manager, Cisco

Ben Fischer, Sr. Product Marketing Manager, Arbor Networks

November 1, 2016

DDoS Attacks Primer

Things You Should Know About DDoS Attacks

- Easy to launch a DDoS attack.
- DDoS attacks are increasing in size, frequency and complexity.
- DDoS attacks are sometimes smoke screen diversions during attack campaigns².
- Enterprises demand increasing for managed DDoS Protection Services.

Did You Know?

\$5

...cost to launch
a DDoS attack

540 Gbps

...DDoS attack
size increasing ¹

74%

...involved DDOS
as a diversion²

42%

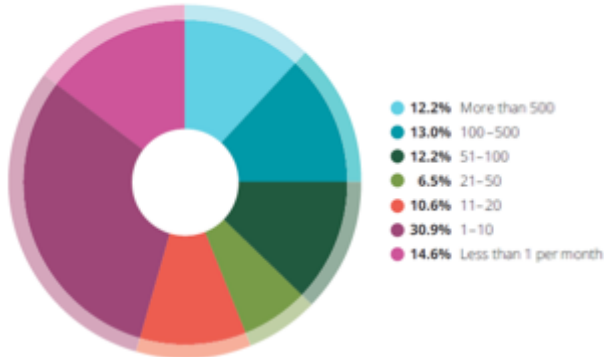
...experienced multi-
vected attacks¹

74%

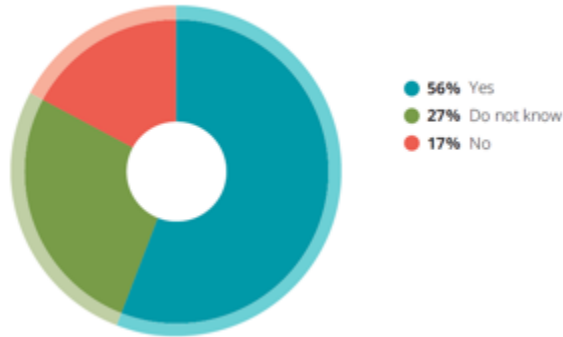
...Increase in demand for
DDoS Protection services¹

DDoS Attacks: A Major Problem Getting Worse

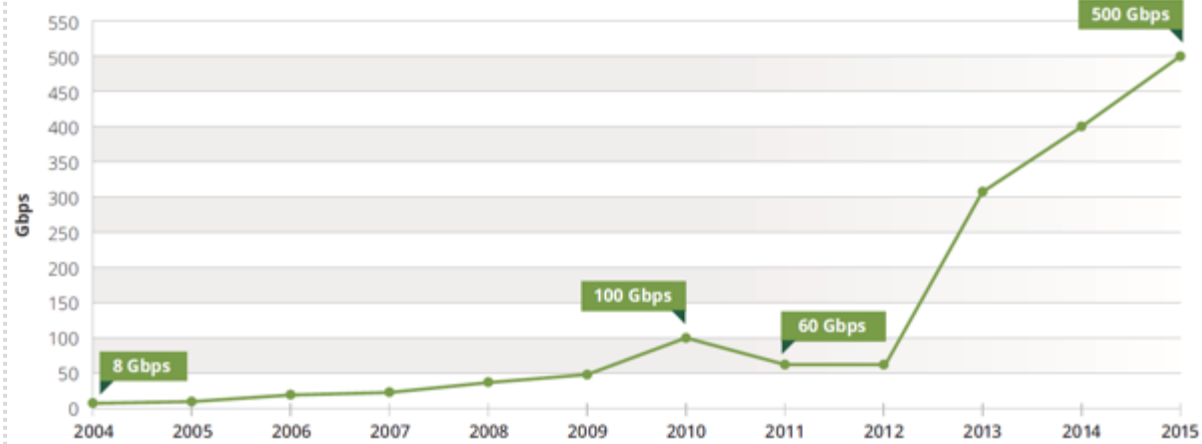
Attack Frequency



Multi-Vector DDoS Attacks



Survey Peak Attack Size Year Over Year



Source: Arbor Networks, Inc. Worldwide Infrastructure Security Report 2016

DDoS Attacks Threaten All Networks

TCP State-Exhaustion Attacks

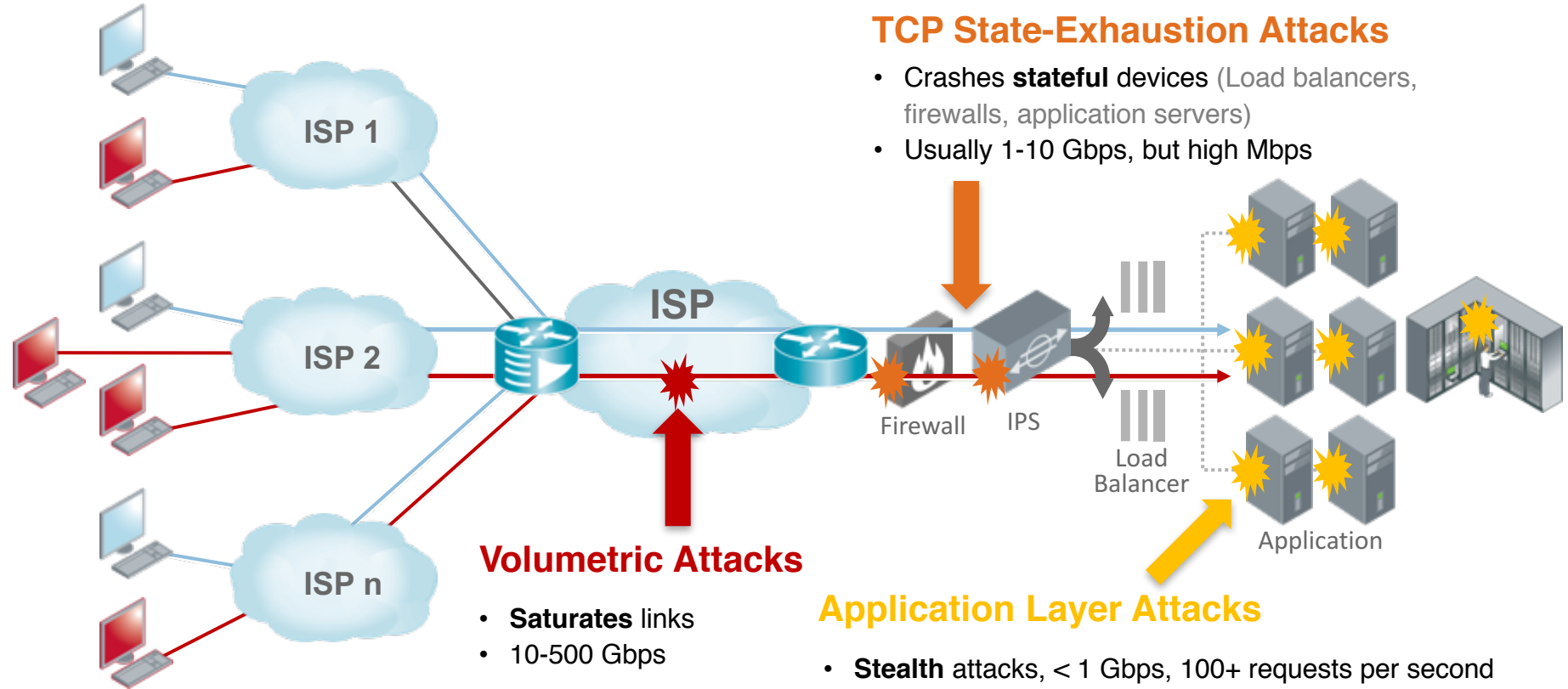
- Crashes **stateful** devices (Load balancers, firewalls, application servers)
- Usually 1-10 Gbps, but high Mbps

Volumetric Attacks

- **Saturates** links
- 10-500 Gbps

Application Layer Attacks

- **Stealth** attacks, < 1 Gbps, 100+ requests per second
- No impact on infrastructure
- Huge load on applications



Demand for DDoS Protection Services

MSSP Market: DDoS Protection Services

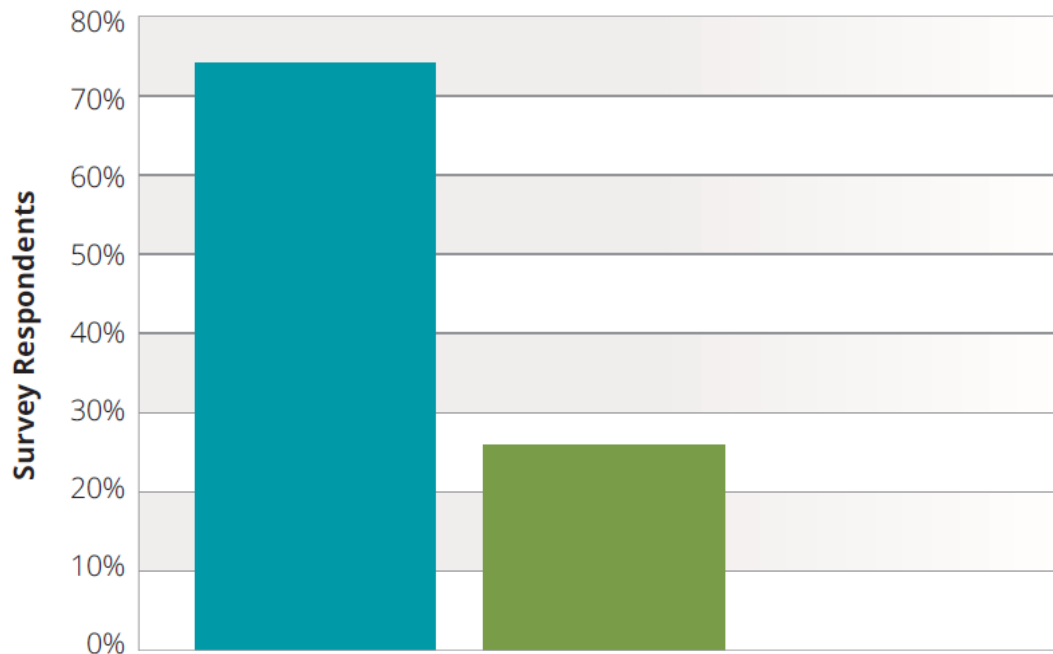
\$2B by 2019 *Estimated by Infonetics*

9% of overall \$22.2B MSSP Market

Estimated by StrateCast

Arbor's 11th WISR Also Shows Increase in Demand

Demand for DDoS Detection/Mitigation Services

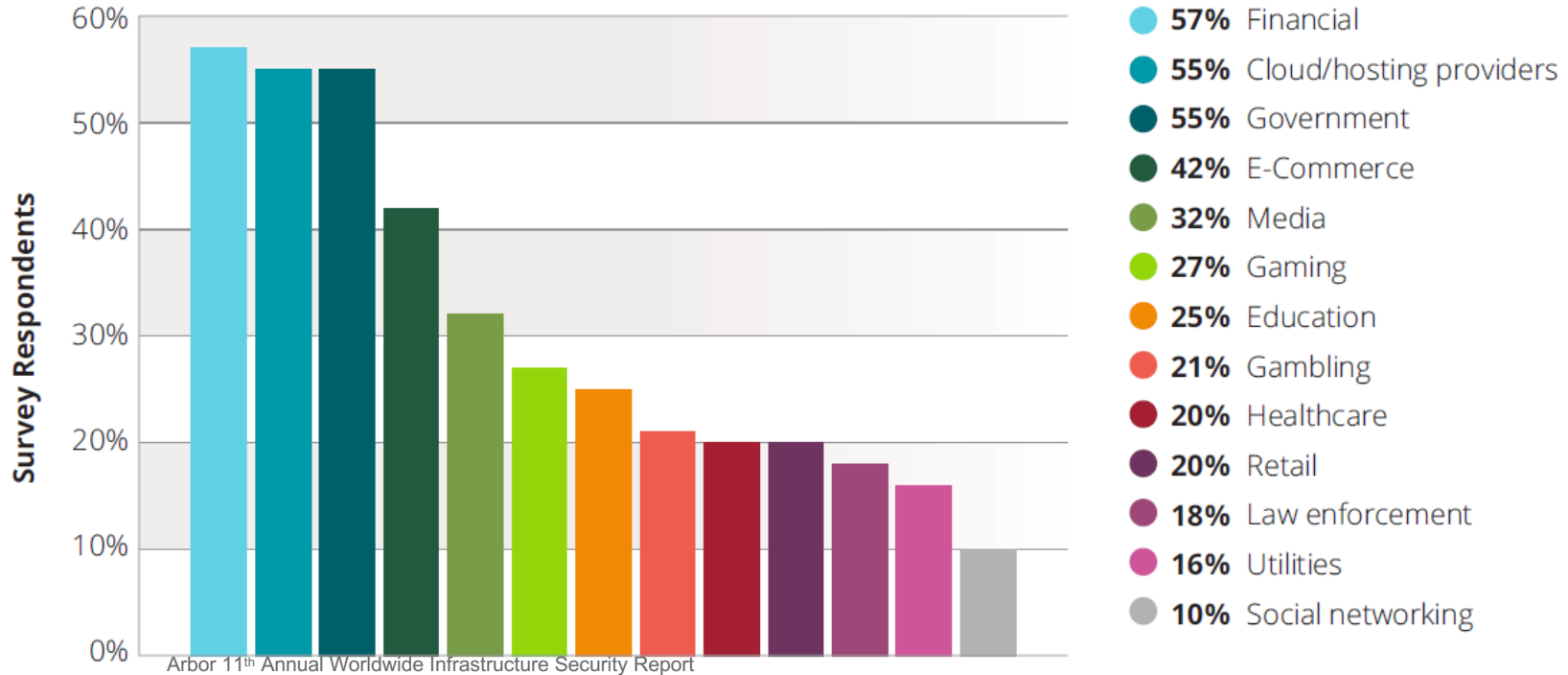


- **74%** Increasing demand from customers
- **26%** The same demand from customers
- **0%** Reduced demand from customers



Large Potential Target Market for Services

Business Verticals for DDoS Services

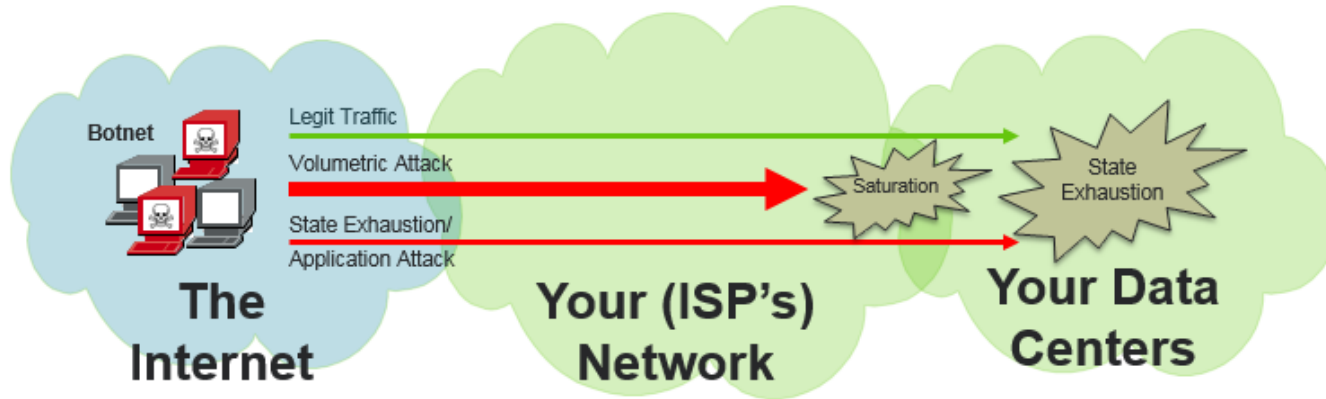


Best of Breed DDoS Protection = Cisco + Arbor Networks

Proven, Trusted DDoS Protection

MODERN DAY DDoS ATTACKS

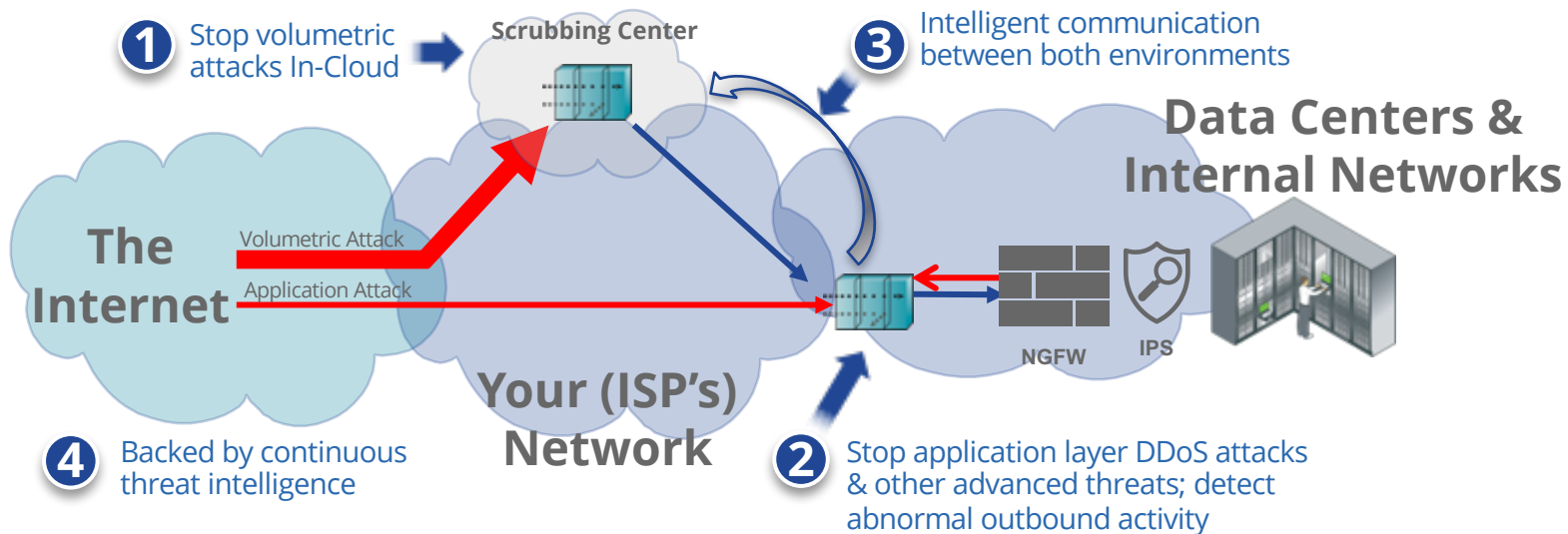
Today's DDoS attacks use a dynamic combination of volumetric, TCP state-exhaustion and application layer attack vectors



There are Industry Best practices exist to stop **all** of these attacks

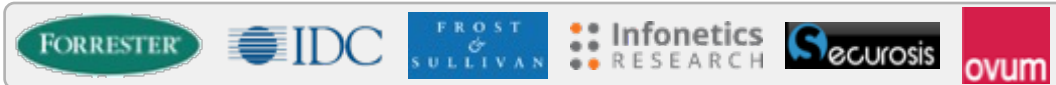
STOPPING DDoS ATTACKS

Layered DDoS Attack Protection



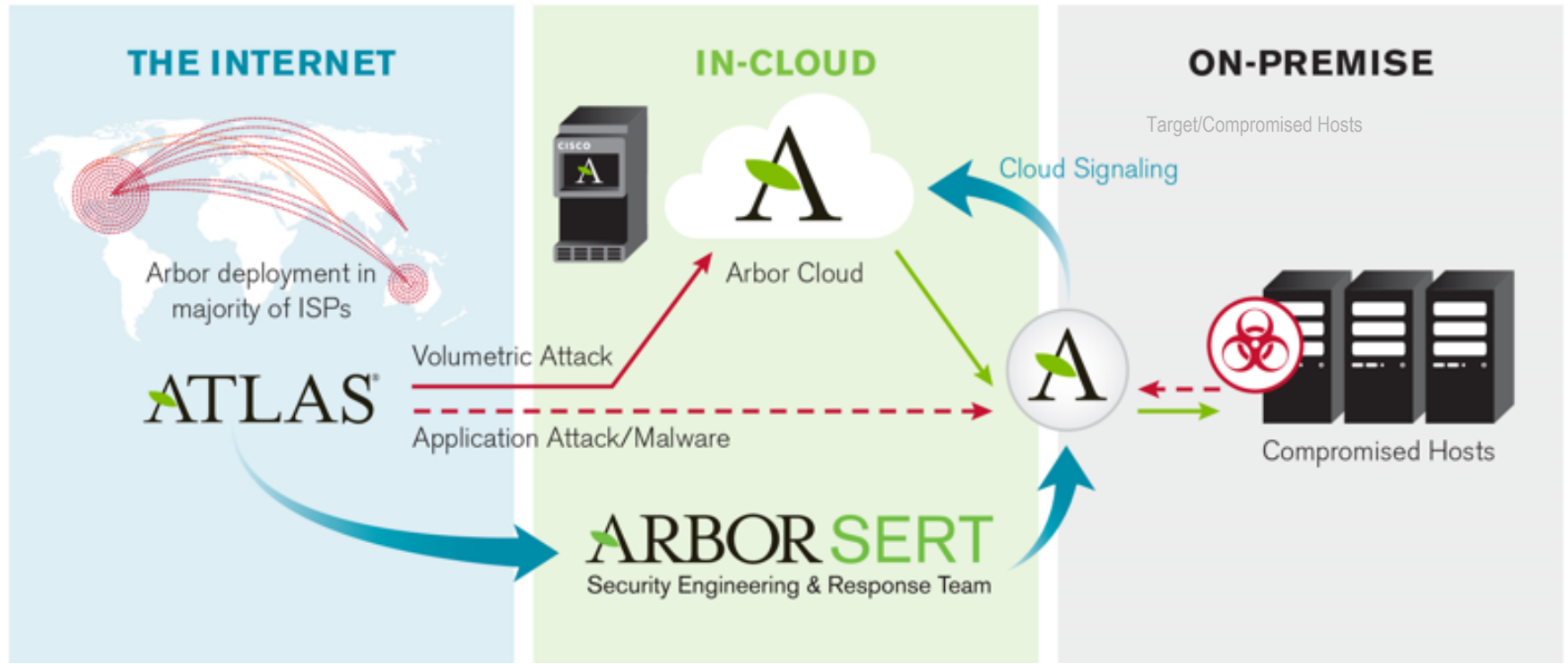
Backed by Continuous Threat Intelligence

A Recommended Industry Best Practice:



ARBOR'S DDoS PROTECTION SOLUTION

Comprehensive DDoS Protection Products & Services



Armed with Global Visibility & Actionable Threat Intelligence

© 2015 Cisco and/or its affiliates. All rights reserved.

Arbor Networks' DDoS Protection Portfolio



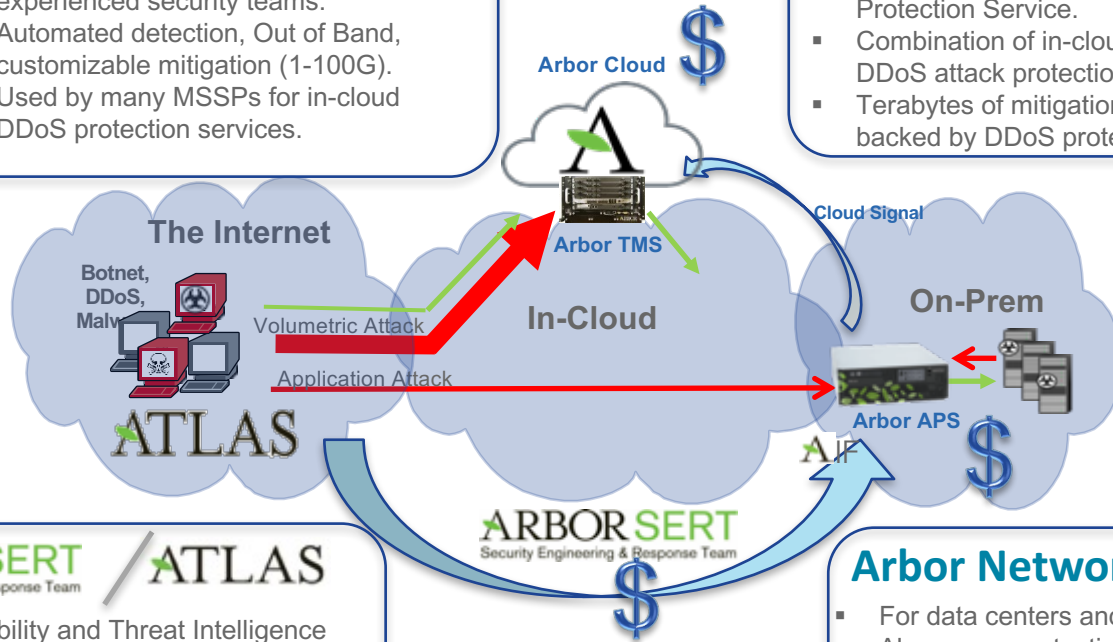
Cisco ASR 9000 Router w/ vDDoS Protection

Arbor Networks SP & TMS

- For more complex networks and experienced security teams.
- Automated detection, Out of Band, customizable mitigation (1-100G).
- Used by many MSSPs for in-cloud DDoS protection services.

Arbor Cloud®

- An ISP Agnostic, Managed DDoS Protection Service.
- Combination of in-cloud and on-prem DDoS attack protection (up to 2TB).
- Terabytes of mitigation capacity, backed by DDoS protection experts.



ARBOR SERT / ATLAS

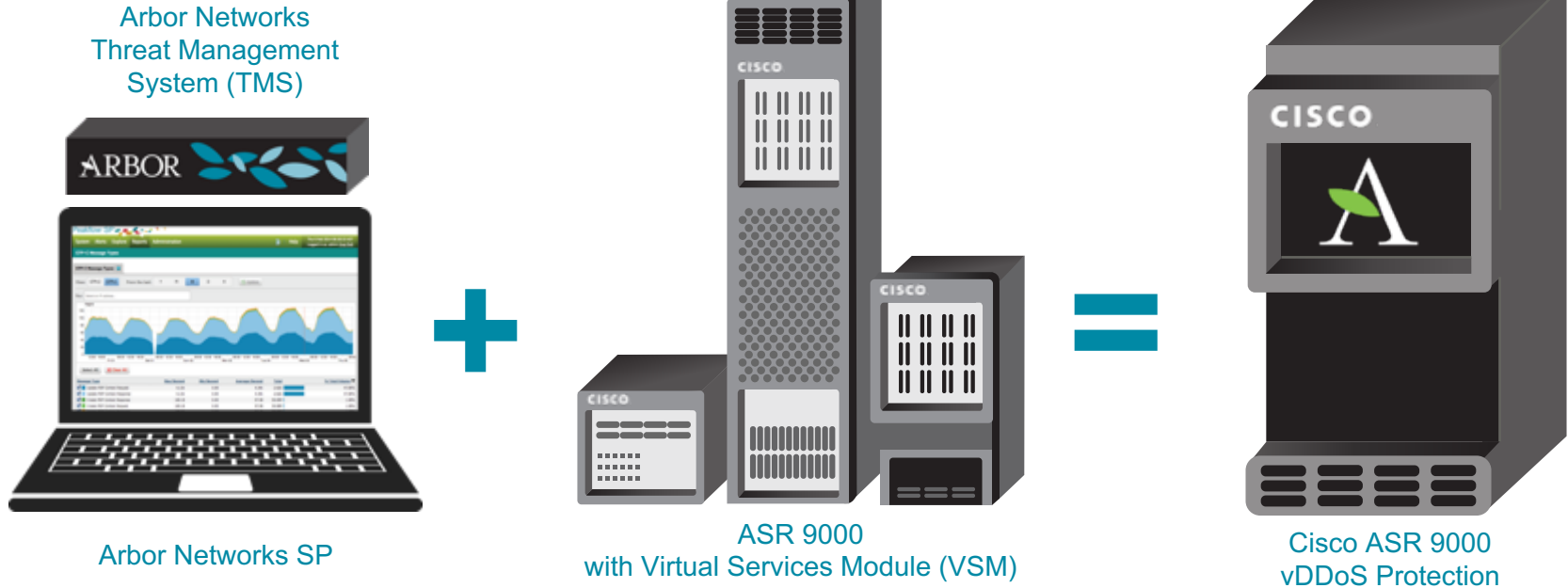
Security Engineering & Response Team

- Global Visibility and Threat Intelligence provide "Situational Awareness".
- ATLAS Intelligence Feed(AIF) arms products with latest, global, actionable, threat intelligence.

Arbor Networks APS

- For data centers and customer premises.
- Always on, protection from (in-bound and outbound) DDoS attacks and advanced threats (sub 100M to 40G).
- Cloud Signaling for large attacks.
- Managed APS

Network Embedded, Virtual DDoS Protection



Up to 60 Gbps Mitigation per VSM

"Powered by Arbor Networks"

Why Use ASR 9000 vDDoS Protection Solution?

- Proven Scalability & Reliability in Largest Tier 1s
 - DDoS attacks detected as fast as 1 second
 - BGP announcement re-route traffic to be scrubbed
- Leverages Your Cisco Infrastructure
- Includes Multi-Tenant Customer Portal

Ask peers and competition: *“Who do you use for DDoS protection?”*

How to Establish Your DDoS Protection Service

Basic Steps

1. Establish Goal of Service
2. Determine Offering(s)
3. Purchase & Install Solution
4. Develop Process
5. Part Numbers & Prices
6. Communicate & Enable Sales

DDoS Protection Services: Potential Packages

Features	Emergency (On-Demand)	Bronze Subscription	Silver Subscription	Gold Subscription
In-cloud: On demand Mitigation of DDoS attacks.	✓			
In-cloud: Proactive Detection of DDoS attacks, reporting.		✓	✓	✓
In-cloud: Proactive Mitigation of DDoS attacks, reporting, customer portal.			✓	✓
CPE based: Proactive DDoS attack detection, and mitigation.				✓
In-cloud + CPE: Proactive Overflow/ Cloud Signaling Mitigation of large DDoS attacks				✓
Price	\$\$\$	\$	\$\$	\$\$\$

How Much Should We Charge?



Heavy Reading – Independent quantitative research and competitive analysis of next-generation hardware and software solutions for service providers and vendors

JUNE 2016

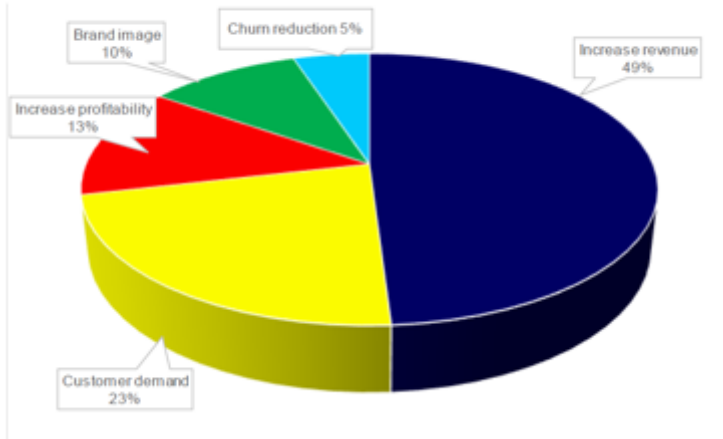
Virtualized Managed Security Services: Monetization For CSPs

KEY FINDINGS
Incremental revenue per customer of 13.5% can be achieved by selling security on top of basic connectivity.
Service providers want differentiated security services as operational simplicity for the enterprise administrator.
Nearly a half of

From a service provider perspective, virtualization promises the potential for a lower cost, more flexible and more distributed security architecture which is better suited to meeting the rapidly evolving landscape of new and emerging cyber threats.

The same tool kit also creates a major new monetization opportunity for service providers to sell virtualized security-as-a-service to business customers. It is the potential to leverage virtualized solutions in pursuit of monetizing security that is the subject of this Heavy Reading study.

Question 7: "What is the most important business driver for offering security services to enterprises?"



Question 8: How much additional revenue does your company expect to generate from offering security services to enterprises compared with their basic spend?

RESPONSE	# OF RESPONDENTS (#95)	% OF ALL RESPONDENTS
At least 25% more than basic spend	10	10.5%
15% to 25% more than basic spend	29	30.5%
10% to 15% more than basic spend	13	13.7%
5% to 10% more than basic spend	36	37.9%
Little or no additional revenue (security is a value-add to lower customer churn)	7	7.4%
TOTAL	95	100%

of respondents: 95

On average service providers expect incremental revenue from selling security-as-a-service of 13.5% on top of spend on basic connectivity. 59% of respondents assume the realistic expectation is 15% or below, 41% believe more than 15% is achievable.

In General, DDoS Protection Services...

- Most DDoS protection services are based around the concepts shown in the next few slides.
- Common Components of Services:
 - In-Cloud vs. On-Prem
 - On-demand vs. Subscription
 - Attack detection vs. mitigation
 - Traffic diversion mechanisms (e.g. DNS / BGP)
 - Access to customer portals, reporting
- Other variances related to SLA, charging mechanism (number of attacks, size of attacks, amount of clean traffic) etc..

Give the Customer The Flexibility to Choose

- Giving the customer options that better match or suit their needs. For example:
 - Mitigation Packs (# of mitigations/month) (e.g.6, 12, 30,50, unlimited)
 - Mitigation Units (e.g. 12, 72 hr)
 - Service based upon average clean bandwidth, not attack size.

- Customer Benefits:
 - Can more easily budget for DDoS Protection. (“avoid a blank check”)
 - Pick the right amount of protection for the right time. (e.g. an e-Commerce company buys more during the holidays)

Customization of Arbor Networks SP Customer Portal

Below this capability group is pre-configured and cannot be edited

- Description**
- Capabilities**
 - Administrative**
 - conf_imp: Import a configuration from disk
 - login_01: Access to the CLI environment
 - sp_admin: SSI and manage SP configuration
 - sp_portal_admin: Administer Portal/SSSI
 - sp_reports_admin: SSI and manage SP reports
 - sp_shell: Shell access to OS
 - sp_ssa: SSI local user and AAA configuration
 - sp_ssa_admin: Install and uninstall software packages
 - Data Access**
 - sp_alerts: View DoS, Traffic, and SP system alerts
 - sp_alerts_dir: Access to DoS Alert reports
 - sp_forensics: View forensics flow information
 - sp_managed_objects_view: Provide basic access to managed object summary information
 - sp_reports_view: View custom report reports
 - sp_restapi: Execute REST API requests
 - sp_restapi: Execute SOAP transactions using Arbor Open API
 - sp_status
 - sp_traffic
 - sp_traffic_agg
 - sp_traffic_fingerprint
 - sp_traffic_host_data
 - sp_traffic_ip_data
 - sp_traffic_ip_location
 - sp_traffic_ip_size
 - sp_traffic_ip_size
 - sp_traffic_ip_size
 - Mitigation**
 - sp_blackhole
 - sp_fingerprinting
 - sp_ips_flowmap
 - sp_ips_flowmap_record
 - sp_ips_mit_record_only
 - sp_ips_mitigation
 - Custom Access**
 - sp_custom1

Arbor Networks SP

Status Alerts Traffic Mitigation Administration The 28 Jul 2016 13:48:15 EDT
 Logged in as: arbor_admin@arbor.com (Log Out)

DoS Host Alert 2155558

Duration: Jul 27 19:36 - Ongoing (18:13) View Scratchpad (0) Mitigate Alert

Summary Traffic Details Routers Annotations Mitigations: None

DETAILS Period: Alert Timeline Traffic View: Network Boundary Update

Severity Level: High Max Severity Percent: 344.0% of 40 Kbps Max Impact of Alert Traffic: 8.5 Gbps/137.7 Kbps Direction: Increasing House Types: UDP Managed Object: VM Target: 141.211.29.101

Alert Traffic: House Types Exceeding Trigger Rate

131.65 Kbps Total Traffic UDP

Status Alerts Traffic Mitigation Administration The 28 Jul 2016 13:48:15 EDT
 Logged in as: arbor_admin@arbor.com (Log Out)

View Applications Summary

View Applications Summary Update

Report Result: "AIMC_TEST", Jul 28 2016, 17:39

Mitigations

Limit: 100 | Search Query: | Managed Objects: Victim 4 | Sort: Start Time | Sort Order: Descending |
 Limit listing to mitigations that allow managed services user access: Off

Graph	Name	Prefixes	Duration	Start Time	User	Type	Last Annotation
	DoS Alert 458344	4.4.4.4/32	0:31 (Ended)	Jul 28 13:50	acockburn	IPv4 TMS	Mitigation stopped. (by acockburn)
	DoS Alert 458325	4.4.4.4/32	0:36 (Ended)	Jul 28 12:04	acockburn	IPv4 TMS	Mitigation stopped. (by acockburn)

Showing 2 Items



Many Considerations

- Market
- Strategy
- Pricing
- Operations
- Finance
- Design
- Deployment
- Launch
- Assessment
- Roadmap



Arbor Resources You Can Rely Upon

- MSSP Consultant
- Consulting Engineer (CE)
- Product Marketing Manager

Arbor-based DDoS Protection Services*



- Today, there are **60+** MSSPs worldwide offering Arbor-based Managed DDoS Protection Services.
 - Approximately 40 offer the combination of In-Cloud and On-Premises.



CISCO

TOMORROW starts here.

More Market Info on DDoS Protection Service Demand

F R O S T & S U L L I V A N



Market
Engineering














DDoS Mitigation Global Market Analysis

New Solutions Accelerate Market Growth

Market Engineering Measurements

Total DDoS Protection Market: Global, 2014

Market Overview

 Market Stage	 Market Revenue	 Market Units/Volume	 Average Price Per Unit	 Market Size for Last Year of Study Period
Growth	\$449.5  (In Millions)	11.5  (‘000s)	\$39.1  (‘000s)	\$977.2  (In Millions)
 Base Year Market Growth Rate	 Compound Annual Growth Rate	 Customer Price Sensitivity	 Degree of Technical Change	 Market Concentration
26.7% 	16.8% (CAGR, 2013-2018)	5  (scale: 1 [low] to 10 [high])	8  (scale: 1 [low] to 10 [high])	76.2%  (market share held by top 3 companies)

Decreasing  Stable  Increasing 

Note: All figures are rounded. The base year is 2014. Source: Frost & Sullivan

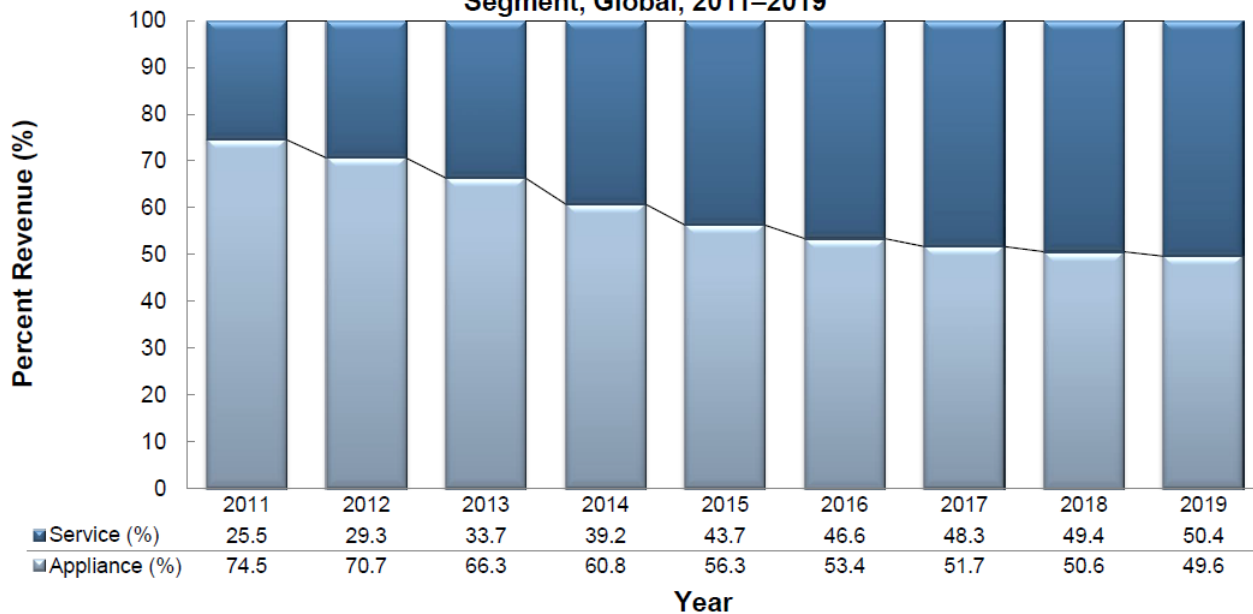
Unit Shipment and Revenue Forecast Discussion

- Demand for DDoS mitigation solutions is accelerating.
- The increase in DDoS mitigation demand is directly related to the [increased frequency](#), [scale](#), and [sophistication of DDoS attacks](#). In particular, awareness of DDoS risk grew prominently in 2014 and will remain at a high level throughout.
- More organizations are being targeted for DDoS attacks, driving demand and new business.
 - Generally, customer awareness of DDoS risk and best practices is strong and continues to improve based on lessons learned from previous attacks, research lab reports, and from case studies of other attacks.
 - Additionally, existing DDoS deployments are being updated to provide comprehensive “hybrid” protection.
- Hosting providers, ISPs, CSPs, and managed security services providers (MSSPs) invest in DDoS mitigation solutions to protect their own networks and also to provide value-adding or premium security services to customers.

Percent Revenue Forecast by Segment

DDoS mitigation services are increasingly popular with new customers.

Total DDoS Protection Market: Percent Revenue Forecast by Segment, Global, 2011–2019



Note: All figures are rounded. The base year is 2014. Source: Frost & Sullivan

The Last Word—Vendor Recommendations

1 DDoS mitigation appliance vendors should offer managed security services to lower barriers to adoption.

2 Service providers including CSPs, ISPs, CDN, and hosting providers, have tremendous amounts of raw network telemetry and threat data. DDoS mitigation vendors should establish intelligence sharing partnerships with service providers in order to improve attack detection times and accuracy.

3 DDoS mitigation vendors should develop hybrid and cloud-based solutions including leveraging technology partnerships, building capabilities in-house, or supporting open standards in order to support enterprise and SMB customers.

The Last Word—Customer Recommendations

1 Businesses should use multiple methods for mitigating DDoS attacks, including basic ACLs and rate-limiting, clean pipes services, and purpose-built hybrid DDoS mitigation solutions.

2 Security professionals should be wary of the network intrusion, fraud, and data theft activities that often coincide with a DDoS attack.

3 Service providers should be considering DDoS mitigation solutions as a means to protect their own networks as well as a potential avenue for new revenue streams.

Growing Demand for Managed Security Services

Key data points:

- Managed security service revenue totaled **\$15.8B in CY14, up 10%** from \$14.4B in CY13; revenue will increase 40% over the next **5 years to \$22.2B in CY19**.
- 54% of CY14 security service revenue came from CPE-based services, with cloud-based offerings contributing 46%. By CY19, CPE revenue will drop to 48% of the total, and cloud-based services will grow to 52%.
- Cloud-based security service revenue totaled \$7.2B in CY14, up 14% from \$6.3B in CY13; the CY14 market will grow 61% over the next 5 years to \$11.6B in CY19; the CY14 market is split as follows: **9% of \$22B = \$1.98B** the market
- 30% of CY14 cloud-based security service revenue is from managed firewall services, 46% from content security, 2% from IDS/IPS, 8% from DDoS mitigation, and the balance (14%) from other security services; by CY19, managed firewall services will constitute 26%, content security 50%, IDS/IPS 2% (flat), **DDoS mitigation 9%**, and other security services 13%.



2015 Network Security Platform Managed Security Service Provider (MSSP) Vendor Rankings for North America

FireEye Makes a Big Move

K05D-74
February 2016



Market Overview (continued)

Total Managed Security Services Market: Market Engineering Measurements, North America, 2015

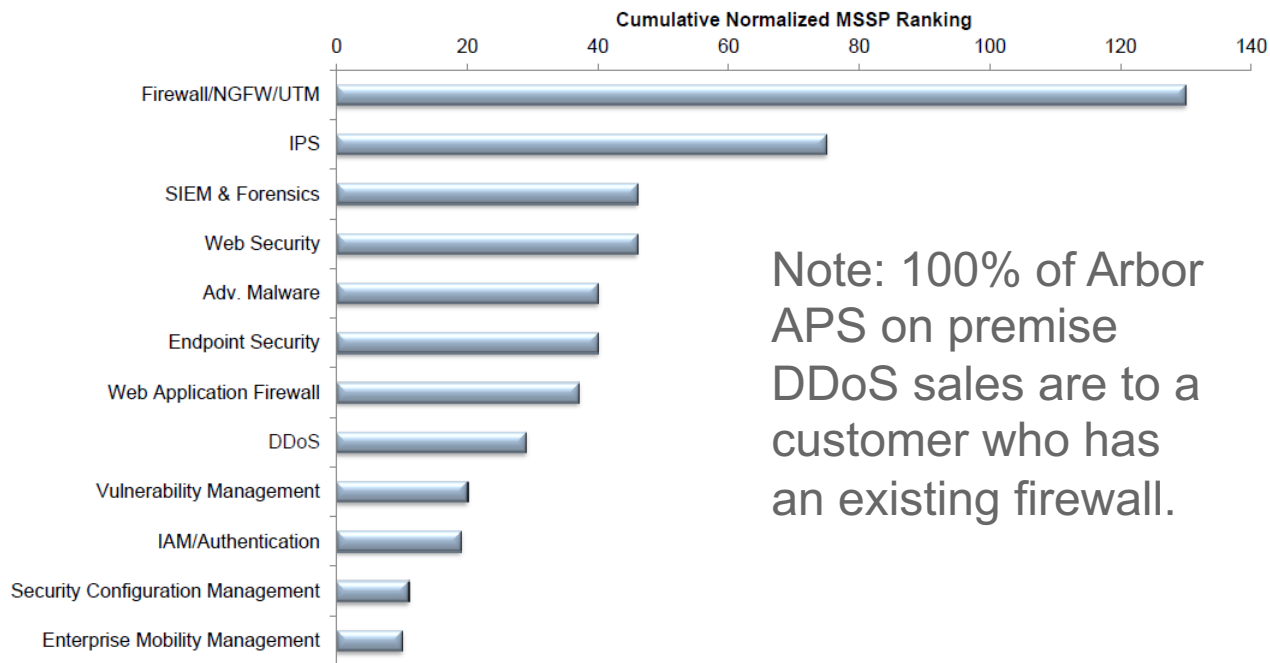
Market Overview



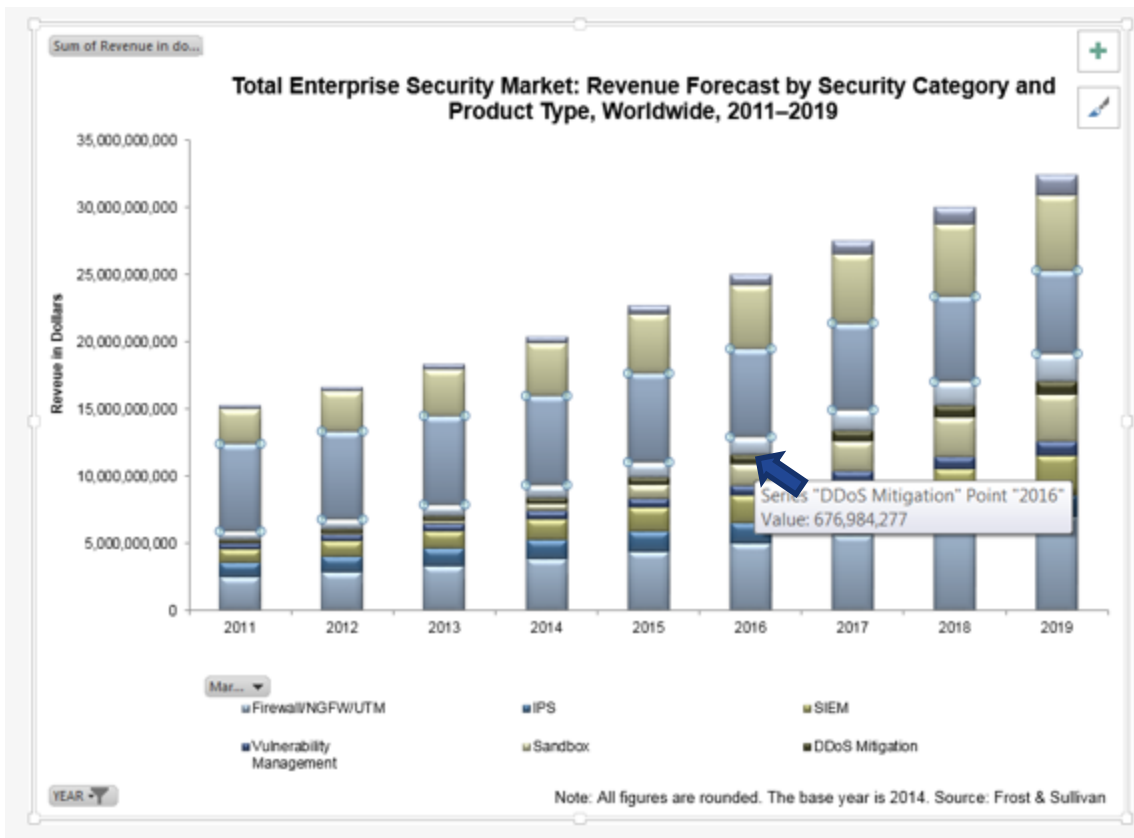
Source: Frost & Sullivan

Cumulative Rankings by Network Security Platform Category

Total Network Security Platform Market: Relative Industry Support for Security Product Category, North America, 2015



Note: 100% of Arbor APS on premise DDoS sales are to a customer who has an existing firewall.



Total Enterprise Security Market: Revenue Forecast by Security Category and Product Type, Worldwide, 2011–2019

Report #K05E-74

Sum of Revenue in dollars		Column Labels								
Row Labels		2011	2012	2013	2014	2015	2016	2017	2018	2019
Device Management										
Endpoint Security	6,514,430,620	6,551,580,385	6,613,202,200	6,633,936,003	6,614,931,194	6,556,291,243	6,458,833,375	6,324,071,197	6,192,120,804	
Internet Property Defense										
DDoS Mitigation	257,900,000	297,330,000	354,830,000	449,460,000	569,007,572	676,984,277	779,528,377	883,328,553	977,210,159	
Knowledge Based Security										
SIEM	994,070,224	1,137,550,231	1,303,587,460	1,505,933,256	1,741,138,723	2,006,899,465	2,299,437,909	2,631,164,290	2,980,777,985	
Vulnerability Management	400,442,414	459,559,508	528,562,421	605,344,702	688,554,337	781,265,838	874,985,753	967,016,624	1,063,077,142	
Security Forensics	629,143,605	730,671,153	837,804,203	967,618,516	1,126,729,799	1,315,415,627	1,523,266,117	1,766,231,019	2,033,951,477	
Network Access & Operations										
Firewall/NGFW/UTM	2,540,483,229	2,885,468,250	3,346,408,023	3,890,675,860	4,436,856,334	5,012,810,543	5,653,783,793	6,293,328,830	6,991,907,974	
Identity & Access Management	2,600,000,000	2,998,000,000	3,480,000,000	3,913,000,000	4,372,500,000	4,769,900,000	5,139,000,000	5,422,400,000	5,632,500,000	
NAC	229,915,000	286,770,000	387,460,000	495,172,000	625,731,515	782,518,900	970,174,400	1,196,385,100	1,468,915,400	
Security Services										
IPS	1,065,800,000	1,199,000,000	1,302,150,000	1,409,851,500	1,488,295,171	1,554,380,012	1,589,524,972	1,602,010,590	1,583,440,045	
Sandbox	30,368,946	103,201,609	229,086,492	536,774,094	1,012,635,035	1,597,731,148	2,238,481,198	2,922,511,712	3,506,631,184	
Grand Total	15,262,554,038	16,649,131,136	18,383,090,799	20,407,765,930	22,676,379,680	25,054,197,052	27,527,015,894	30,008,447,916	32,430,532,169	

All Values are in \$

Note: All figures are rounded. The base year is 2014. Source: Frost & Sullivan



Examples of Arbor Networks Based Managed DDoS Protection Services

Example: For Free or Fee?

... Our *DDoS Protection service is available with minor set-up fees and for a flat monthly fee. Customers will have to pay an additional mitigation charge when under attack...*

... *There are no set-up fees because customers are using their own edge device to detect an attack. When an attack is detected a customer goes to the carrier's DDoS Portal to redirect traffic to a shared "scrubbing facility"...*

Example: Mitigation vs. Detection

Note: Prices are not actuals. Simply meant to show relative difference between prices.

Pricing/Licensing: Flat monthly fee starting at \$3,500 per month for mitigation and \$1,500 per month for detection

MSSP's DoS capabilities, which date back to its acquisition, began with regionalized DoS mitigation in 2004. Over time, MSSP extended its offering to include detection capabilities and global availability backed by a 100 percent uptime service-level agreement (SLA). Upgrades that are currently under way will expand MSSP's mitigation capability to 60 GB in each of two network backbones with another 40 GB of capacity in a third. MSSP's mitigation capabilities are uniquely granular. While many providers require customers to reroute a block of address space (a/24) through their mitigation or scrubbing capability, MSSP can do this down to a single IP address. As a result, customers needn't reroute all traffic on the same network segment as the attack target (for example, rerouting both e-mail and Web site traffic when only the Web site is under attack). MSSP DoS protection also has no variable fee; even if customers face repeated, large volume attacks, they pay the same monthly rate.

Example: Tiers of Service

The screenshot shows a website's navigation menu with 'Infrastructure Services' selected. A sidebar lists various services, with 'Security' highlighted in blue. A callout box with a torn-edge effect contains text about security services, with a red circle around the word 'comprehensive' and a red arrow pointing to the 'Security' link in the sidebar.

Home Advantages Industries **Infrastructure Services** Solutions

Infrastructure Services

- Cloud
- Managed Hosting
- Colocation
- Network
- Security**
- Virtualized Security Services
- In-the-Cloud Security Services
- Threat Management
- Log Management
- DDoS Protection
- Firewall
- Intrusion Detection
- Email Security Solutions
- File Integrity Monitor
- Incident Management Systems
- Security Professional Services

Security

Round-the-Clock Enterprise Security. Constant Fire Incident Response.

The rising risk of attacks, their increased complexity when the escalating costs of protecting their systems against them. It's companies are turning to us for management of their IT the decision easy. We minimize your exposure to common threats your system and application vulnerabilities, and provide 24/7 and response – usually at a lower cost than it would take for yourself.

Trust Our Technology. Depend on Our Expert Security Professionals. Rest Easier.

We're flexible. Whether you want security protection delivered in a Savvis data center, or "in the cloud," we've got you covered.

We're comprehensive. Start with a basic firewall. Add anti-spam and anti-virus protection. Move to complete security coverage that includes threat management, distributed denial of service (DDoS) attack mitigation, and log management. Whatever your needs, we have the security services to address them.

We're cost-effective. Security technologies are expensive, and constantly changing. Just keeping your equipment and software current can take a huge bite out of your IT budget. Add the cost of recruiting and retaining skilled personnel, and you'll likely to suffer severe sticker shock. Now ask us for a quote. Once you do the math, we're your

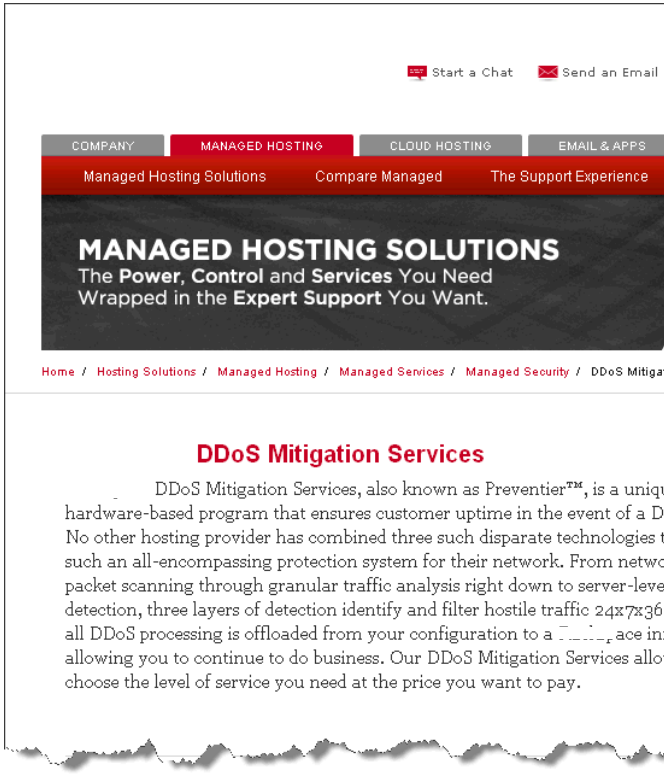
Maximize Uptime, Minimize Costs.

Because the : Network-Based DDoS Mitigation Service is based "in the cloud," you don't have to buy any equipment or software upfront. For a predictable — and affordable — fee, you get access to the advanced DDoS detection and filtering equipment located on s' Tier 1 Internet network backbone, which stretches to more than 40 countries and serves approximately 25 percent of the world's Internet traffic.

Two DDoS Mitigation Service options are available:

- **Basic Service:** You contact the Response Center when you suspect a DDoS attack is underway. Your traffic will be placed into "protect mode," which means that legitimate transactions will continue to be processed while malicious traffic is stopped.
- **Enhanced Service:** Our world-class Managed Security Team monitors your network 24/7 to detect attacks on your behalf, and place your traffic into protect mode

Example: Good Use of Arbor SP Features



The screenshot shows the Rackspace Managed Hosting Solutions website. At the top, there are links for 'Start a Chat' and 'Send an Email'. Below that is a navigation bar with categories: COMPANY, MANAGED HOSTING, CLOUD HOSTING, and EMAIL & APPS. Under MANAGED HOSTING, there are sub-links: Managed Hosting Solutions, Compare Managed, and The Support Experience. The main heading is 'MANAGED HOSTING SOLUTIONS' with the tagline 'The Power, Control and Services You Need Wrapped in the Expert Support You Want.' At the bottom of the screenshot, there is a breadcrumb trail: Home / Hosting Solutions / Managed Hosting / Managed Services / Managed Security / DDoS Mitigation.

DDoS Mitigation Services

DDoS Mitigation Services, also known as Preventer™, is a unique hardware-based program that ensures customer uptime in the event of a DDoS attack. No other hosting provider has combined three such disparate technologies into such an all-encompassing protection system for their network. From network packet scanning through granular traffic analysis right down to server-level detection, three layers of detection identify and filter hostile traffic. 24x7x365 all DDoS processing is offloaded from your configuration to a Rackspace facility, allowing you to continue to do business. Our DDoS Mitigation Services also allow you to choose the level of service you need at the price you want to pay.



How It Works

TIER 1: Network-Level Traffic Monitoring & Analysis

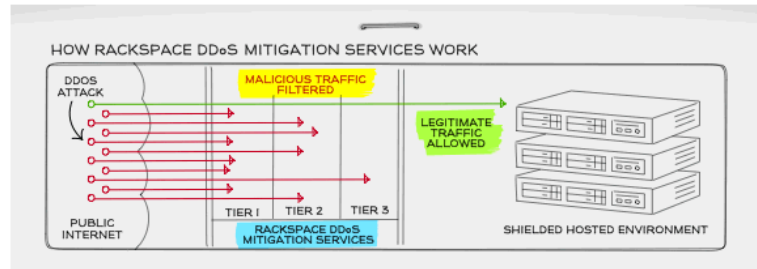
The service starts by monitoring all traffic entering Rackspace network. Sophisticated Intrusion Detection technology, capable of handling over 30 million packets per second, examines each and every incoming packet for signs of malicious activity. Meanwhile, Cisco NetFlow statistics perform granular traffic analysis of source and destination IP addresses, protocol information, flow information, and traffic volume. DDoS Mitigation Services report this information to Rackspace Network Operations Center (NOC) experts, who use it to make routing decisions for best performance and to provide information on the attack type, source, protocol, and duration to any affected customers.

TIER 2: Server-level Anomaly Detection

The service also searches for anomalies on a per-server basis. It does this 2 ways. The Premium offering analyzes your server's traffic patterns to learn about "normal" network behavior and combining the results with port usage information to create a profile of your server's usual traffic. The service then monitors the traffic on your server, constantly comparing it to this profile and looking for unusual behavior. If it detects an anomaly, the malicious traffic is immediately filtered and blocked. The other Rackspace DDoS Mitigation Services offerings use a standard profile to determine any anomalies.

TIER 3: Traffic Filtering & Re-Routing

Finally, if malicious activity is detected, the service acts quickly, routing suspicious traffic through a "sanitation engine", which uses multiple DDoS detection methods to filter out and divert malicious traffic. All legitimate traffic is then forwarded to the intended destination servers, which are able to serve clients entirely unaffected by the ongoing DDoS attack.



Use of only Arbor/ Cisco vSP product and numerous reports.

Use of only Arbor/ Cisco vSP product anomaly detection.

Use of only Arbor / Cisco vSP and Arbor TMS/ Cisco vDDoS products.

Example: Good Website

Contact Us Careers Login

WHO WE ARE WHAT WE DO WHY UPTIME UNIVERSITY BLOG

What We Do: Managed Services

MANAGED FIREWALL MANAGED ROUTING MANAGED NETWORK MONITORING MANAGED DNS/PROTECTION

MANAGED DDoS PROTECTION

DDoS attacks are becoming more common and any business with Internet is a target.

Managed DDoS Protection service monitors, reports and offers optional mitigation for Distributed Denial of Service attacks that can disrupt critical business services such as Internet, email and websites.

What is a DDoS attack?

The goal of this type of cyberattack is to overwhelm the resources available to a network, application or service so that legitimate users are denied access.

How does a DDoS attack work?

To carry out an attack, hackers recruit virus-infected computers to act as zombies. They then maliciously attribute robotic armies, or botnets, to attack your network's digital resources such as computers and servers. That's what you see happening in the attack map at the bottom of this page. When your assets are overwhelmed, the attack cuts off legitimate users, denying them access to your business and its services.

Digital Attack Map

The map below is a snapshot in time of DDoS attacks happening throughout the world. The tool is a collaboration between Google Ideas and Arbor Networks. Click on the map to see a live version of reports of anonymous attack traffic, outages and historic trends.

SEE THE MAP LIVE www.digitalattackmap.com

- ### Resources
- Federal framework can be big help in cybersecurity planning
 - 7 cybersecurity targets to protect, monitor in 2016
 - 4 common business cyber infections and how to prevent them

- ### Recent Blogs
- Attackers have stepped up their game. Businesses must, too.
 - Risks to democracy should make cybersecurity a higher priority
 - Surveillance Center never takes time off; clients can rest easier

How to stop the attacks?

offers multiple levels of protection as an additional service to our Internet subscribers. In each package, our Managed DDoS Protection identifies the malicious traffic and has the ability to stop the bots through mitigation or deploying countermeasures on your Internet pipe. Customers can receive alerts, 24x7 support and scheduled reports depending on the level of service.

Features	Reporting Only	Reporting & Mitigation	
		Standard	Premier
Monitoring & Notification			
DDoS Monitoring	✓	✓	✓
24x7 Support		✓	✓
Customer Portal		✓	✓
Weekly Summary Report	✓	✓	✓
Monthly Summary Report	✓	✓	✓
Email Notification of High Alerts	✓	✓	✓
Phone Notification of High Alerts			✓
Managed Objects			
Managed Objects Included	1	1	3
Mitigation Types			
Manual Mitigation	✓	✓	✓
Auto Mitigation			✓
Tiered Protection			
1 Gb		✓	✓
2 Gb		✓	✓
3 Gb		✓	✓
Overage Per Mb		✓	✓
Additional Managed Objects		✓	✓

Example: Use of Arbor Threat Intelligence

iomart products partner about us g cloud investors news contact 0800

Protection from the network up

iomart has invested in the latest advance threat protection to secure its infrastructure against cyber attacks. Denial-of-Service (DDoS) attacks are on the rise and have evolved into complex and overwhelming security challenges for

Network Protection Solutions Recap

Peakflow from Arbor Networks provides comprehensive network visibility and reporting capabilities to help you detect and understand availability threats, and improve traffic engineering, peering relationships and service performance.

- Increased Network Visibility, Stronger Security, Improved Services
- Comprehensive DDoS Detection and Analysis – Real-time reporting of critical network traffic, services and applications to proactively protect against DDoS attacks, including comprehensive protection for dual-stack IPv4/IPv6 infrastructure.
- Application Layer Intelligence and Protection – applications such as voice, video, data, messaging, file sharing, Web, email and more, profiled for their behaviour and acted upon.
- Intelligent Traffic Engineering – IPv4 and IPv6 traffic modelling across your entire network
- Fully managed by iomart or self managed by you
- Pricing based upon monthly subscription and agreed protected transit fee

Leveraging Threat Intelligence from ATLAS/ASERT

Digital Attack Map - Top daily DDoS attacks worldwide

iomart uses the Arbor Peakflow® SP platform to proactively defend itself from malicious threats such as botnets and volumetric and application-layer distributed denial of service (DDoS) attacks.

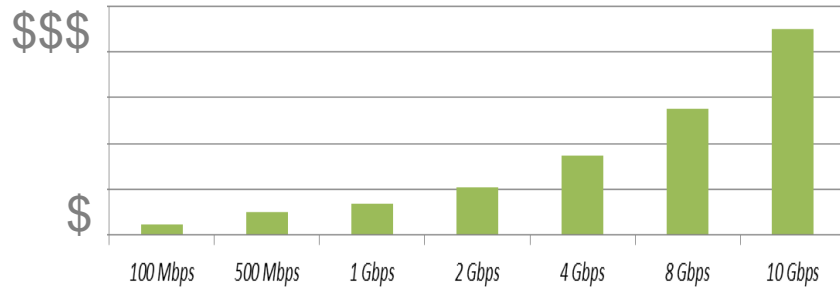
Example: Based Upon Clean Bandwidth

Cloud DDoS Protection Plans

Imperva offers flexible 1, 2 and 3-year standby and automatic service plans to meet specific business needs. The standby plan can be enabled when under attack. The automatic plan is a continuous service that can be purchased in conjunction with the Imperva Cloud WAF service.

	Standby Plan 1 Gbps	Standby Plan 2 Gbps	Automatic Plan 1 Gbps	Automatic Plan 2 Gbps
Bandwidth:	1 Gbps	2 Gbps	1 Gbps	2 Gbps
Burstable Bandwidth Limit:	2 Gbps	4 Gbps	2 Gbps	4 Gbps
Managed DDoS Service:	Included	Included	Included	Included
Additional 100 Mbps Bandwidth, per Month:	Optional	Optional	Optional	Optional
Websites Included with Service:	1	1	All	All
Additional Websites:	Optional	Optional	Included	Included

Example: Arbor Cloud DDoS Protection for Enterprise



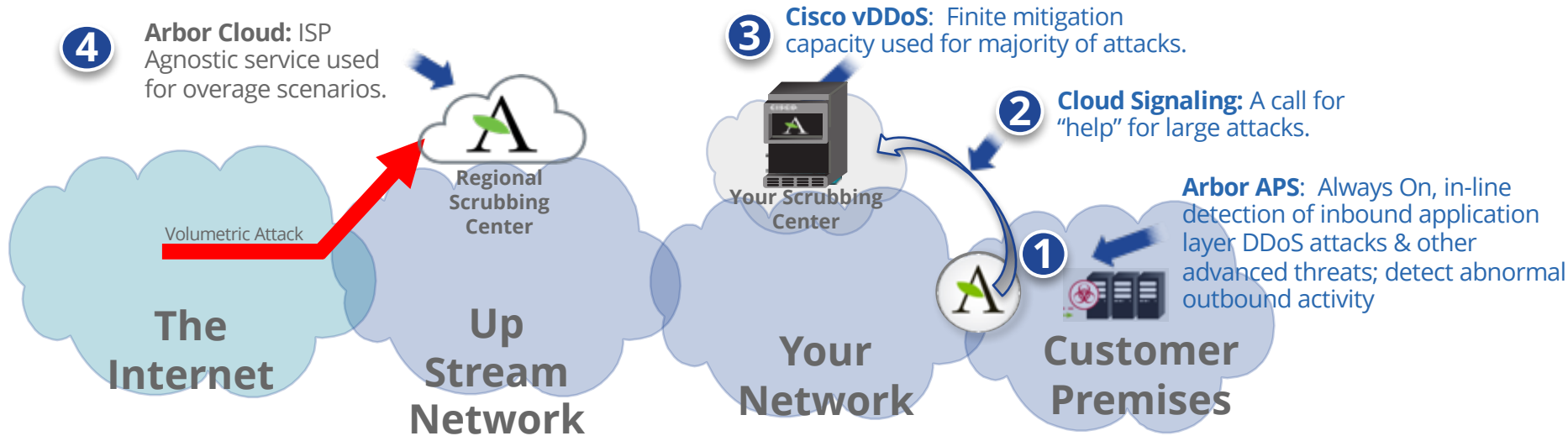
▪ An Example of Putting It All Together:

- No initial provisioning fees
- Prices based upon normal amount of Clean Traffic; sold as a annual subscription, billed monthly.
- Includes 12 mitigations per year; extra mitigation packs can be purchased separately.
- Mitigation = 72 hour window
- BGP option includes 1 /24 subnet and 1 GRE destination; extra /24 and GRE tunnels sold separately.
- DNS option includes 5 hostnames; additional hosts sold separately.
- ON-premise Arbor APS with Cloud Signaling sold separately.

Case Study: Arbor Cloud for Service Providers

Customer	US Data Center Operator. Services include: Custom data center, Colo, Cloud Services, Managed Hosting, Internet Connectivity.
Arbor Solution	Combination of Peakflow SP, TMS 2310 and Arbor Cloud DDoS Protection for SP (Small Tier, 7 BGP/GRE locations, 3Yr)
Background / Driver	<ul style="list-style-type: none">▪ Some of their DCs were experiencing DDoS attacks.▪ After multiple failed attempts to justify a product only solution (i.e. TMS too expensive) – settled on hybrid solution:▪ TMS for “Surgical Mitigation” (i.e. 5-10G, for most attacks)▪ Arbor Cloud as an “insurance policy” for larger attacks.

Extending In-Cloud Mitigation Capacity



- *Arbor Cloud for Service Providers*
 - An ISP Agnostic Managed DDoS Protection Service
 - Offering 2 TBps of Global Scrubbing (4 regional locations)
 - Use as an insurance policy for scenarios when attacks exceed mitigation capacity of local TMS.