IHS TECHNOLOGY

DDoS Prevention Appliances

Biannual Market Tracker: Regional, H1 2016

Excerpts

13 June 2016

ihs.com

For the half-year ended
31 March 2016

Contents

Exhibits

Top Takeaways: DDoS Prevention Appliances Near $150M in 1Q16, Up 30% YoY

Key observations from the last 6 months:

- The market was flat QoQ in 1Q16 as if fairly typical for the first calendar quarter, but YoY revenue growth was strong; this is a sign of the maturation of the DDoS mitigation market—it's now starting to fall into normal seasonal growth trends.

- There is an opportunity to sell on-premises DDoS mitigation solutions to deal with the cluster of lower-bandwidth attacks plaguing many networks, then hand off larger attacks to a dedicated cloud scrubbing provider; this is driving adoption of hybrid solutions and sales of hardware at the lower end of the market, including large enterprises, small/medium hosting/cloud providers, and tier 2/3 service providers who in the past relied on their upstream bandwidth providers for DDoS mitigation.

- Arbor maintained its market share leadership position, holding 44.7% of worldwide revenue; Arbor has led this market for a decade and continues to stay on top of emerging trends like hybrid DDoS mitigation deployments, managed services, on-premises solutions for a wide range of deployment scenarios, and virtual appliances.

Market Background and Key Drivers

DDoS prevention appliances are the first line of defense for most service providers and large enterprises around the globe looking to protect themselves from brute-force attacks on network or resource availability, and with the unprecedented number, size, and coverage of DDoS attacks since the floodgates opens in 2008, vendors who build DDoS prevention solutions have seen and continue to see a significant increase in demand. This report covers actuals for 4Q15 and 1Q16.

Verizon's Data Breach Investigations Report (DBIR) had an entire section dedicated to DDoS attacks in 2015, and added to it in 2016. The total number of attacks is skyrocketing, application layer attacks are becoming more common, and even volumetric attacks are evolving. Volumetric attacks are bifurcating into very high velocity/bandwidth attacks (59G and up, and 15 million pps and up), and lower-bandwidth attacks (15G/3 million pps). This has significance for everyone, but particularly large enterprises, mid-sized cloud and hosting providers, and smaller telecom providers (tier 2 and 3/regional providers).

We cover broad market drivers later in this report, but put simply, the key drivers for increased investment in DDoS prevention solutions include:

- The increasing volume of **highly visible attacks**, including a mix of politically motivated attacks, state-sponsored electronic warfare, social activism, organized crime, and good old fashioned pointless mischief and mayhem, driven by the easy availability of bots/botnets for hire and easily distributed crowd-sourced attack tools

- Increasing number of **sophisticated application-layer attacks** like R.U.D.Y and Slowloris that some DDoS detection and mitigation infrastructure can’t identify and block, forcing companies to make new investments in DDoS solutions

- Emergence of new varieties of **amplification attacks** like the DNS amplification attack aimed at Spamhaus in 2013 that topped 300G, and the NTP amplification attack earlier this year that topped 400G; these attacks are pushing the boundaries of mitigation performance

- **Internet traffic growth**, which has driven major carriers to upgrade their backbone infrastructure to increase capacity, driving a need for increased capacity DDoS prevention solutions; Cisco predicts IP traffic will pass the zettabyte threshold in 2016 and reach 2.3ZB by 2020, with a 2015-2020 CAGR for IP traffic of 22%.

- **Enterprise and tier 2/3 carrier and mid-sized hosting provider demand for on-premises solutions** is growing every day even though conventional wisdom says that most large enterprises and regional carriers and mid-sized hosting companies should deploy cloud-based solutions for DDoS mitigation; there are many enterprise environments where data simply cannot leave privately owned networks and data centers to be scrubbed in the cloud (mostly for compliance reasons), and many smaller regional SPs and hosting providers are looking to leverage on-premises tools to lower operating costs and generate revenue from customers for customized services

- **Data center consolidation,** data center upgrades, and the rollout of the cloud infrastructure that will underpin the next generation of cloud services; large data centers and cloud providers are highly visible targets who must protect their own infrastructure and the customers who trust them to host data and applications; in the last 5 years the scale and architecture of most medium and large data centers have changed significantly, and large enterprises and hosting/cloud providers need DDoS solutions with improved performance, faster physical interfaces, and advanced detection and mitigation technologies

- **Mobile network upgrades,** which many mobile providers are making to deliver 3G and 4G services and meet the demand for broadband data for mobile devices, are forcing providers to add new layers of network protection and increase their overall security processing capacity; backhaul networks alone are adding orders of magnitude more capacity, driving the need for new DDoS solutions

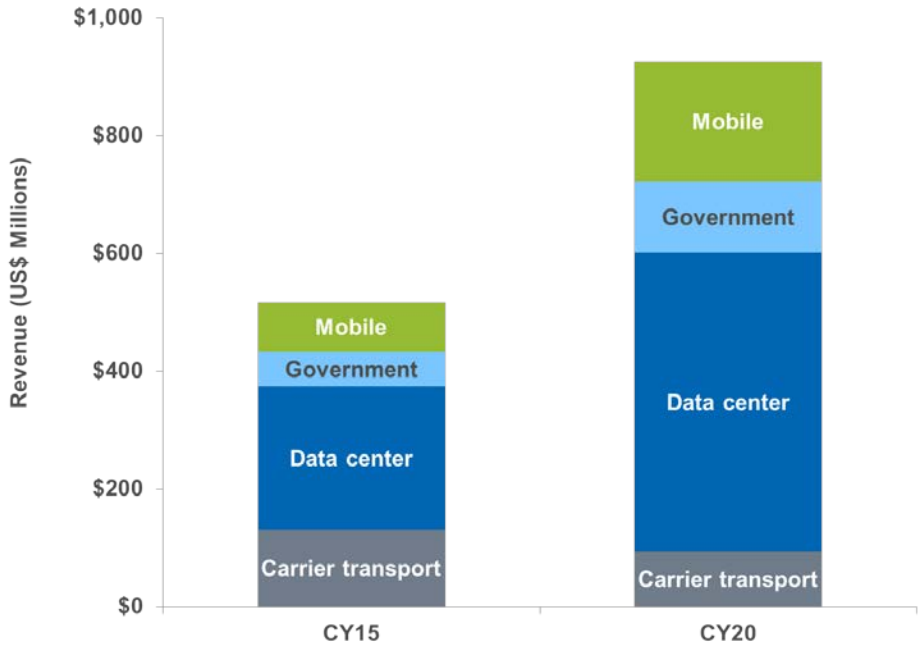
- **Managed DDoS mitigation services;** in addition to purchasing DDoS solutions to protect their own infrastructure, many carriers around the globe are buying DDoS products to build out managed services for their customers, and specialized hosted DDoS service providers (like Prolexic) are gaining popularity with enterprise customers looking for DDoS prevention but lacking the expertise or capital to deploy their own; we now track these services in our *Cloud and CPE Managed Security Services* report

- **SDN and NFV** are pervasive trends in network and telecom infrastructure, and they will eventually touch all areas of security; though virtual appliance solutions for DDoS mitigation aren’t widely available, it’s not hard to imagine (particularly in an NFV context) a world where DDoS mitigation can be dynamically provisioned via software; Radware announced an SDN and NFV strategy for carriers that included DDoS functionality in February 2014, and there will be more announcements

Long-Term Forecast: Data Center Deployments Maintain Lead, Mobile Passes Carrier Transport by 2018

Exhibit 1 shows annual revenue for the DDoS prevention appliance market split by the 4 deployment locations we track, as well as the YoY growth for the total market (the gray line). DDoS prevention appliance market growth will stay in the double-digit percentages through 2017, after which some of the larger infrastructure upgrades in mobile and data center start to slow down a bit. Service providers are investigating and begin deployment of lower cost (and virtualized) solutions and DDoS solutions integrated with other security and networking products—this will begin to chip away at the lower end of the enterprise and service provider space, dropping the price of DDoS prevention.

Exhibit 1 **Worldwide DDoS Prevention Appliance Revenue by Deployment Location**

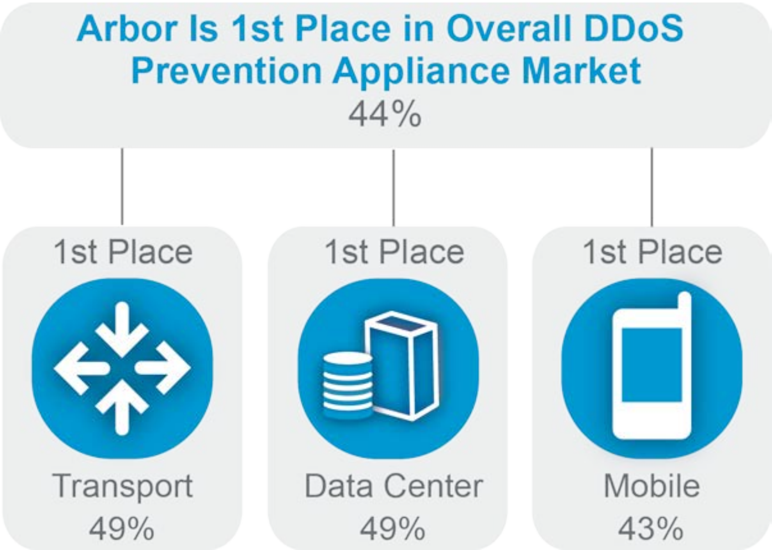


Source: IHS © 2016 IHS

Manufacturers and Market Share Analysis: Arbor Networks Maintains Lead

In 1Q16 total DDoS prevention appliance revenue, Arbor ranks first with 46% (up 2.9 points from 2Q15); Arbor maintains a strong leadership position despite having a wide range of challengers. The introduction of their hybrid cloud services, fully managed services, a refreshed on-premises offering, and advanced threat detection and analytics will help them grow their overall business revenue by tapping into fast-growing markets. Their transition to some subscription revenue is already impacting their appliance revenue (starting in 4Q14), but the overall business remains quite strong.

Exhibit 2 Worldwide DDoS Prevention Quarterly Revenue Market Share



Source: IHS © 2016 IHS

Demand-Side Data

We verify our supply-side forecasts with our demand-side research, and work closely with vendors, service providers, chip and component manufacturers, and the channel to gather and validate actual data and market trends. This gives us a thorough, accurate picture of the market. We collected the following demand-side data over the last 12–18 months.

In *Data Center Security Strategies and Vendor Leadership: North American Enterprise Survey,* our April 2016 survey of 151 medium and large organizations in North America that operate their own data centers, we found that:

- Three-fourths of respondents are driven to deploy new security solutions because they need to upgrade to high speed network interfaces on their security appliances to match the upgrades done in their switching infrastructure.
- Protection against new DDoS attacks is a primary security investment driver for 74% of respondents, up significantly from last year.
- 46% of respondents plan to increase spending on DDoS prevention products by March 2016.

In *Cloud and Data Center Security Strategies and Vendor Leadership: Global Service Provider Survey,* our December 2015 survey of 26 major service providers around the globe, we found that:

- 62% of respondents are driven to deploy new security solutions to handle new DDoS attacks.
- 88% will build their own DDoS mitigation infrastructure or use a hybrid model.
- Firewall and DDoS mitigation top the list of threat mitigation platforms respondents plan to make the largest investments in over the next year.
- Despite being a narrowly focused DDoS vendor, Arbor is seen as a top security vendor overall by large service providers, and the top DDoS mitigation solution supplier.

Contact

Jeff Wilson
Senior Research Director,
Cybersecurity Technology
+1 (408) 583.3337
jeff.wilson@ihs.com

IHS Customer Care:

Americas: +1 800 IHS CARE (+1 800 447 2273); CustomerCare@ihs.com
Europe, Middle East, and Africa: +44 (0) 1344 328 300; Customer.Support@ihs.com
Asia and the Pacific Rim: +604 291 3600; SupportAPAC@ihs.com