IHS TECHNOLOGY

DDoS Prevention Appliances

Biannual Market Tracker: Regional, H2 2016

13 December 2016

ihs.com

For the half-year ended
30 September 2016

Contents

Market Size and Forecast Analysis: Market up 33% YoY in 3Q16 1
DDoS Risk Profile 3
Manufacturers and Market Share Analysis: Arbor Networks Maintains Lead 4

Market Size and Forecast Analysis: Market up 33% YoY in 3Q16

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.

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). The Mirai IoT botnet, and DDoS attacks associated with IoT botnets in general have been the hottest issue this year on the attack front; massive attacks fueled by billions or trillions of connected devices are definitely the future, and the entire industry is investing and gearing up solutions to protect against this new generation of attacks.

The adoption driver for hybrid solutions and sales of hardware at the lower end of the market will be the opportunity to make a capital investment in on-premises DDoS mitigation to deal with the cluster of lower-bandwidth attacks, then hand off larger attacks to a dedicated cloud provider. These new hardware sales are among the primary drivers behind our aggressive forecast through 2020.

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

- The buildout of massive new **IoT botnets** like Mirai and LizardStresser give us a glimpse of the future of attacks; these botnets are already capable of launching sustained attacks >500G, with the first Terabit attack arriving in February of 2016.

- **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

DDoS Risk Profile

There are 3 basic types of issues form the risk profile that most enterprises and service providers use to determine when (and how much) to invest in a given security solutions. The ability of a solution to address these risks is the primary determining factor in the financial success and long-term viability of the commercial market for that solution. The three categories of risk are:

- **Loss of data** is the first risk category; typical data-loss prevention solutions range from data encryption to intrusion prevention and access control. For an organization to invest in security to prevent loss of data, they must have valuable data to protect, and they must understand the monetary value of that data; as a result, investing in security to prevent data loss is a priority for a subset of all organizations around the world.

- The second risk category includes **regulatory or compliance** repercussions for not protecting electronic assets; in the absence of regulations or compliance, many companies may not choose to invest in security solutions for their valuable data; many vertical markets are affected by regulations (such as healthcare and finance), and there are other regulations that impact broader groups of organizations (PCI, SOX, or GLBA in the US). Even non-regulated industries can face compliance issues that impact security spending, as many companies are required to demonstrate a certain level of security for business licensing or insurance purposes; regardless, the threat of repercussions for not being compliant drives many organizations around the globe to invest in network security.

- The final risk category is the negative impact of **availability/downtime** problems; in our 2007 study The Costs of Network Security Attacks: North America 2007 we found that organizations lose an average of 0.5% to 2.5% of annual revenue due to security-related downtime. When online retailers go down, they lose revenue; when trading systems are attacked and traders cannot trade, they lose revenue. Businesses that have their websites defaced or forced out of commission can suffer intangible damage associated with brand and image. This risk is horizontal, as companies of all type and size are plagued by downtime associated with security attacks regardless of the value of their data or regulatory or compliance requirements.

DDoS prevention is only peripherally involved in protecting against loss of data, and as for regulatory/compliance requirements, in cases where availability is mandated as part of the regulation, then a DDoS solution can be deployed, but where DDoS really matters is loss due to downtime/lack of availability. DDoS attacks, are by name, an attempt to deny a service; that can be any number of services, denied for any purpose an attacker can dream up.

DDoS attacks are simple: flood a resource with traffic until that resource overloads and becomes non-functional. Some attacks require vulnerabilities in the end system, while others simply require brute force. The availability of rental botnets and simple tools has made it simple for anyone to launch an attack, and the scale of the attacks is growing rapidly. Most of the technical innovation in DDoS prevention is around meeting the ever-increasing performance requirements driven by large attacks.

Manufacturers and Market Share Analysis: Arbor Networks Maintains Lead

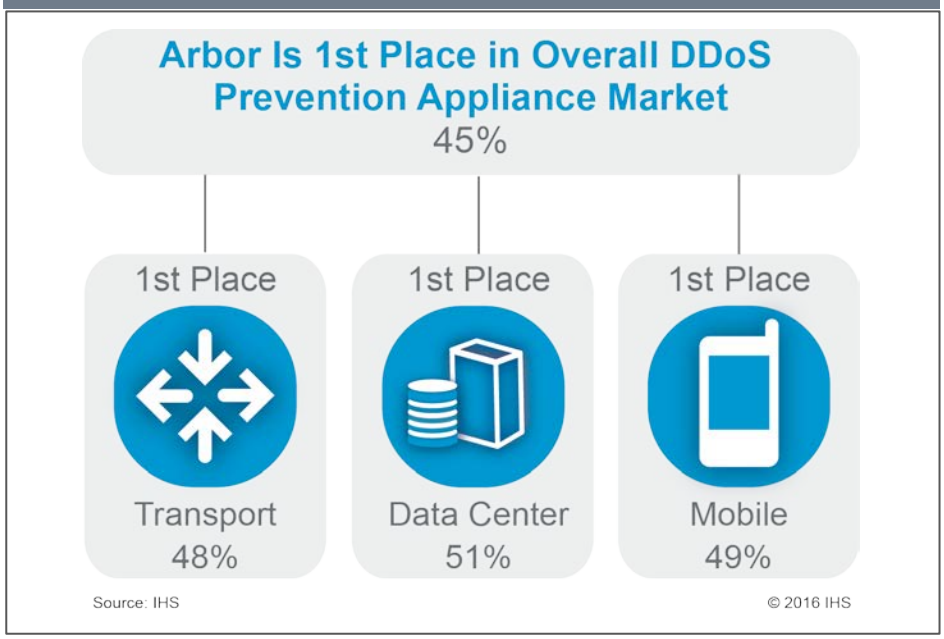
In 3Q16, total DDoS prevention appliance revenue, Arbor ranks first with 45.3% (up 2 points from 2Q16), followed by Radware at 7.4%. Arbor managed strong double-digit YoY growth 2Q16 and 3Q16 and grew its leadership position despite having a wide range of challengers, from focused product vendors in adjace'nt markets (like A10, who just jumped into the game in early 2014, and F5) to large established networking and security vendors (like Fortinet, who is putting increasing focus on DDoS mitigation).

Arbor turned in excellent YoY growth performance in 2Q16 and 3Q16, but it's always difficult for a dominant leader (owning roughly half of the market) to outgrow the market consistently, especially when there are many regional opportunities that go directly to regional players. It's much easier to grow revenue at 20%+ QoQ when starting from a base of $3M or less—that said, Arbor's revenue grew >20% YoY in 2Q16 and 3Q16. The introduction Arbor's hybrid cloud services, fully managed services, a refreshed on-premises offering, and advanced threat detection and analytics helped it grow its overall business revenue by tapping into fast-growing markets. Arbor was able to add over 120 new customers in the last 6 months, across a wide range of segments (enterprise, traditional service provider, government, and cloud/hosting), which helped drive this exceptional growth.

Arbor's biggest competition will come from dominant technology trends (virtualization, the integration of DDoS into other platforms, and the move to hybrid/cloud services).

Arbor leads overall, but their lead is less dominant once we look beyond the carrier transport sub-market. They have significant share in data center as well, and addressed a product hole with the release of their Arbor APS solution, but several other vendors have a strong focus on data center and good share position in that segment.

DDoS Prevention Worldwide 3Q16 Revenue Market Share



Contact

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