DDoS Prevention Appliances: Excerpts

Biannual Market Tracker: H1 2020

Publication Date: 23 June 2020

Jeff Wilson
Senior Research Director,
Cybersecurity Technology

Table of Contents

List of Figures

Market size and forecast analysis: COVID-19 strikes in 1Q20, but capacity increases drive long-term growth

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. With the unprecedented number, size, and coverage of DDoS attacks since the floodgates opened in 2008, vendors who build DDoS prevention solutions have seen and continue to see a significant increase in demand. This report covers actuals for 4Q19 and 1Q20.

Note: This document is an excerpt; please contact Omdia for the full report.

Verizon's Data Breach Investigations Report (DBIR) had an entire section dedicated to DDoS attacks for the first time in 2015 and has added to it every year since then. The total number of attacks is skyrocketing, application layer attacks are common, and even volumetric attacks are evolving. The Mirai IoT botnet—and the IoT botnets that continue to appear since Mirai—have shaken the world awake and forced everyone from the smallest business to the largest service provider to seriously reexamine their DDoS mitigation plans. In 2019, NETSCOUT threat intelligence tracked 23,000 DDoS attacks per day, and noted a 64% increase in attacks on mobile networks. Massive attacks fueled by billions of connected devices are the future, and the entire industry is investing and gearing up solutions to protect against this new generation of attacks. The move to 5G infrastructure will only compound the problems, greatly increasing the bandwidth for connected mobile devices (and the volume of attack traffic they can generate).

The world is nearly six months into rolling responses to COVID-19 as the pandemic ripples across the globe. This is an ever-changing situation, and it will have short- and long-term effects on all kinds of spending. The initial impact involved supply chain issues that mostly impacted chips, components, and appliances coming from affected areas. Entire cities and regions are under quarantine, large group events have been canceled, and the live concert business, professional sports, and entertainment in general are having a hard time finding a path forward. The travel industry is in free fall as governments restrict movement, businesses implement stricter travel policies, and tourism is hit hard. It is obvious that COVID-19 will significantly slow economic activity across the world—at least on a temporary basis—as people stay put and spend less. The OECD reported real GDP decline of 1.8% in 1Q20.

It remains difficult to accurately assess the impact of COVID-19 on the solutions tracked in this report. Loss of revenue and the current state of the stock and commodities markets will have longer lasting effects on the economy. Omdia expects short-term shortfalls in revenue as some large project purchasing is pushed from the 1Q20–3Q20 timeframe out to 3Q20–3Q21. The long-term outlook has increased in 2022 and 2023. The shift to working from home (both temporary and permanent) and reliance on public network infrastructure are only increasing in the wake of COVID-19, which actually increases the long-term opportunity for selling DDOS mitigation infrastructure.

Hackers ramp up activity in times of chaos, so even though IT budgets will tighten, security will be a priority. Companies will accelerate their move to the cloud to ensure their IT infrastructure is

dynamic, and security will have to follow, which will stimulate growth in all areas of cloud security (including virtual appliances of all sorts). There was also some rush spending in 1Q20, and some is projected for 2Q20 as companies needed to increase capacity for certain applications and networks and had to buy additional security capacity to keep up; this happened in SSL VPN but was also reported by some firewall, IPS, and DDoS mitigation vendors. Most vendors that saw a negative impact on core hardware products already have cloud and SaaS solutions in place to capture the revenue shift, so when Omdia examined revised vendor outlooks for 2020, there were no massive changes in overall expectations (although every piece of guidance was incredibly cautious).

Hybrid solutions and sales of hardware at the lower end of the market to help deal with application layer, low-bandwidth volumetric attacks, and edge network solutions are driving significant revenue for many DDoS mitigation product vendors. These new enterprise sales, along with network capacity upgrades to prepare for 5G (and other bandwidth increases in the backbone of the internet and cloud service providers), new high-bandwidth attacks, and strong customer demand for managed solutions from hosting providers and carriers are the primary drivers behind Omdia's aggressive forecast.

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

- The impact of **COVID-19** on the global economy and on technology spending of all types e.g. the increased need to defend VPN concentrators from attack given increased home-working.
- 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** that some DDoS detection and mitigation infrastructure can't identify and block. This is forcing companies to make new investments in DDoS solutions that can react more quickly, and which be configured to focus on their specific application traffic profiles.
- The emergence of **amplification attacks** like the DNS amplification attack aimed at Spamhaus in 2013 that topped 300G, as well as follow-on amplification attacks exploiting a variety of protocols that have driven attacks over 1T; 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 of over 500G, with the first Terabit attack arriving in February of 2016, a nearly 2tbps attack recorded in mid-2018, and massive application layer attacks hitting in mid-2019.
- **Internet traffic growth** has driven major carriers to upgrade their backbone infrastructure to increase capacity, driving a need for increased capacity DDoS prevention solutions; by 2022, there will be 4.8 billion internet users and 28.5 billion networked devices and connections

- **Enterprise and Tier 2 and 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 that require a faster response than many cloud services offer, or 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 five 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 additional 4G services and upgrade to 5G, are forcing providers to add new layers of network protection and increase their overall security processing capacity significantly. Backhaul networks alone are adding orders of magnitude more capacity, driving the need for new DDoS solutions, and 5G-enabled mobile devices will dramatically increase how much attack traffic a 5G mobile bot can generate (and will enable the connection of untold millions of devices).
- **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; Omdia now tracks these services in the *Cloud and CPE Managed Security Services Market Report*.
- **SDN and NFV** are pervasive trends in network and telecom infrastructure, and they will eventually touch all areas of security; although 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; large carriers are already looking for more flexible DDoS mitigation solutions that can be deployed on off-the-shelf hardware, across their network edge .

DDoS risk profile

There are three 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: 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.

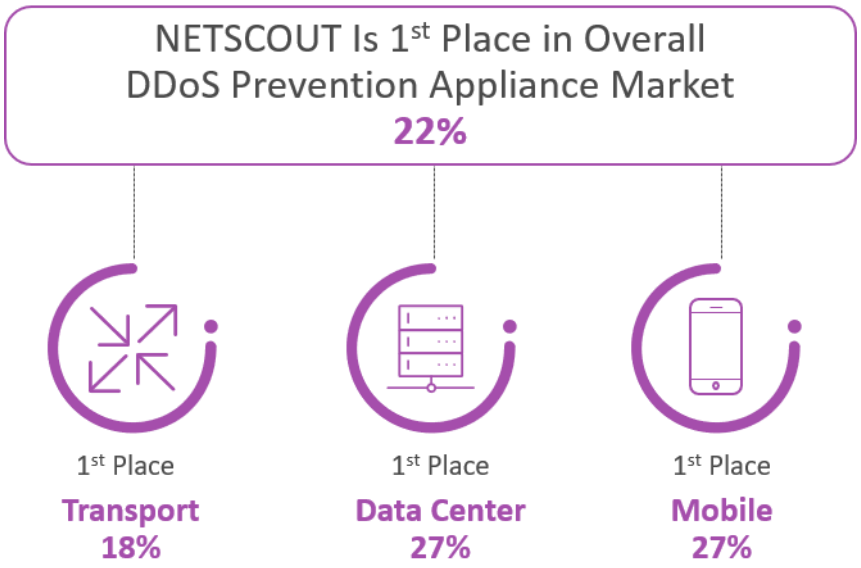
DDoS attacks are simple: flood a resource with traffic until that resource overloads and becomes non-functional. Some attacks require vulnerabilities in the end system, while others simply require brute force. The availability of rental botnets and simple tools has made it simple for anyone to launch an attack, and the scale of the attacks is growing rapidly. Much of the technical innovation in DDoS prevention is around meeting the ever-increasing performance requirements driven by large attacks, but this has shifted as attacks become more sophisticated and vendors are focusing on intelligent automation to reduce operational overhead.

Manufacturers and market share analysis: NETSCOUT maintains the lead

In 1Q20 total DDoS prevention appliance revenue, NETSCOUT ranked first with 22% market share.

NETSCOUT is facing a wide variety of challengers, but is holding onto the leadership position and doubling down on security more broadly, which provides great exposure for the NETSCOUT DDoS solutions. NETSCOUT notes a significant architectural trend toward deploying smaller/virtual DDoS mitigation solutions at the edge, which their software version of TMS can support on COTS hardware with flexible licensing. It has also been successful in growing its enterprise DDoS mitigation business, which now represents a significant share of its overall revenue. Arbor's solutions are now wholly integrated into the overall NETSCOUT portfolio, and integrations (like Sightline with Sentinel) allow it to do some interesting smart/orchestrated mitigation at the edge.

Figure 1: DDoS prevention worldwide quarterly revenue market share



Author

Jeff Wilson, Senior Research Director, Cybersecurity Technology

askananalyst@omdia.com

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com