MARKET ANALYSIS

Worldwide DDoS Prevention Products and Services 2013–2017 Forecast

John Grady  Christian A. Christiansen
Curtis Price  Christina Richmond

IN THIS EXCERPT

The content for this excerpt was taken directly from the IDC Market Analysis: Worldwide DDoS Prevention Products and Services 2013–2017 Forecast by John Grady, Christian A. Christiansen, Curtis Price and Christina Richmond (Doc # 239954). All or parts of the following sections are included in this excerpt: IDC Opinion, In This Study, Situation Overview, Future Outlook, Essential Guidance, and Synopsis. Also included is Figure 1 and Tables 1 and 2.

IDC OPINION

While much of the focus in the security market centers on newer threats from emerging technologies such as cloud, mobility, and targeted malware, an issue that has been around for well over a decade is seeing renewed attention in recent months. Denial of service (DoS) and distributed denial of service (DDoS) attacks were thrust back into the mainstream consciousness in 2012 by high-profile attacks on the world’s leading financial firms. This wave of politically motivated attacks was just the most recent iteration of a phenomenon that gained widespread notoriety in 2010 when supporters of WikiLeaks brought down the Web sites of Visa, MasterCard, Amazon, and PayPal. The 2010 and 2012 attacks both served to reinforce the fact that any business is vulnerable to a denial of service attack and what organizations stand to lose in terms of both revenue and brand equity. Further, these recent instances highlighted the newest scenario of attack where DDoS is used as a diversionary tactic while advanced malware and vulnerability exploitation simultaneously target sites for financial information and intellectual property. In 2012, IDC saw a sharp increase in attacks’ frequency, bandwidth volume, and applications orientation. With the prevalence of these attacks on the rise, organizations need to be aware of, and take steps to protect their infrastructure from, the advanced methods today’s attackers use. IDC believes that:

- The worldwide market for DDoS prevention solutions will grow by a compound annual growth rate (CAGR) of 18.2% from 2012 through 2017 and reach $870 million.

- Volumetric attacks will continue to be the predominate type of DDoS attacks because of the relative ease with which botnets can send a bandwidth flood in excess of what most enterprise infrastructures can handle.

- Despite volumetric-based attacks remaining most popular, more advanced hybrid attacks that include application layer and encrypted traffic in addition to
volumetric methods will grow, helping drive growth in the on-premise equipment market throughout the forecast period.

- Hybrid defense scenarios (on-premise equipment married with cloud services) will become more prevalent as organizations seek to defend against all vectors of DDoS attacks and as solution providers and product vendors work more closely together to deliver joint solutions.

**IN THIS STUDY**

**Methodology**

See the Methodology in the Learn More section for a description of the forecasting and analysis methodology employed in this study.

In addition, please note the following:

- This forecast sizes the market for dedicated DDoS prevention products and services. Some of the main vendors in the market and their offerings are listed in the Situation Overview section.

- This market sizing does not consider revenue from embedded DDoS prevention features in firewalls, unified threat management appliances, next-generation firewalls, routers, and switches.

- For more information on IDC’s definitions and methodology, see IDC’s *Worldwide Security Products Taxonomy, 2012* (IDC #235288, June 2012) or IDC’s *Software Taxonomy, 2012* (IDC #235401, June 2012).

- Research for this document was conducted in late 2012 and early 2013. Some information contained in this study was derived from IDC’s Worldwide Security Appliance Tracker as of September 27, 2012, and IDC’s Software Market Forecaster database as of November 15, 2012.

- Numbers in this document may not be exact due to rounding.
SITUATION OVERVIEW

History of DDoS and Current Attack Landscape

The methods and motivations behind denial of service and distributed denial of service attacks have evolved noticeably over the course of the past decade. Originally, DDoS attacks centered more on brute force tactics, with little focus on stealth or circumventing defenses. An attacker would gain control of a system with an abundance of bandwidth and use it to quickly starve the target of network resources through ping floods, fragmented ICMP packets, or other methods. As attack exploits evolved and resources became more distributed, motivations changed as well. Attack under the threat of extortion became more prevalent, especially toward gaming, gambling, or other targets with less reputable business models.

In 2010, "hacktivism" began to play a much more prominent role in notable DDoS attacks. The rise of rentable botnets and easily accessible code (e.g., Low Orbit Ion Cannon [LOIC]) helped exacerbate the problem, as it became even easier for a single moderately skilled person to launch an attack against any organization with which he/she had an ideological difference. The "anonymous" attacks against the Church of Scientology and multiple organizations due to the WikiLeaks and Megaupload litigation showcased what a skilled group was capable of and how large the DDoS threat had become.

Today’s attacks take on a variety of patterns and sizes. Again, because of the ease of botnet access, large attacks are common and 20Gbps+ attacks have been reported. Layers 3 and 4 ICMP, SYN, and UDP flood attacks are straightforward enough to launch via a botnet. But at the same time, many attacks have become more sophisticated and stealthy. Layer 7 application attacks are much more targeted and often consist of "legitimate" traffic, making them more difficult to detect. Additionally, application layer DDoS attacks require fewer resources to launch, a less important point with the accessibility of botnets, but an interesting one nonetheless. Yet application layer attacks have not begun to outpace network layer attacks in prevalence. The reason may be due to a number of factors: organizations are increasingly focusing on application layer defense, forcing attackers to return to brute force; the ease with which a high-bandwidth attack can be successfully launched equates to the difficulty in hiding the IP addresses instigating the attack once it is discovered.

Many recent attacks feature a combination of the two methods. A DDoS offensive may begin with a volumetric attack, then target servers to starve resources, and finally use an HTTP flood to target an application. Taking it a step further, DDoS has been increasingly used as a diversionary tactic to draw attention away from the true attack target. In this case, an organization under attack may be forced to shut down some of its in-line defenses, thus allowing the attacker to exfiltrate sensitive information. A recent example of this strategy is the $900,000 cyberheist conducted against Ascent Builders, a construction firm based in Sacramento, California, through its financial institution, Bank of the West. This cyberheist-plus-DDoS approach is
becoming increasingly tied to DDoS attacks initiated to distract attention from high-dollar thefts. Advanced hybrid attacks and SSL-based encrypted attacks will cause the most disruption for organizations.

**Defense Scenarios**

To defend against DDoS attacks, there are three mitigation solutions to consider:

- **On-premise.** Technically, many on-premise devices offer denial of service protection including routers and switches, intrusion prevention solutions, and firewalls. These products typically lose the ability to adequately mitigate a denial of service attack when it is over 1Gbps or at the application layer. While some organizations still rely on these built-in defenses, this study focuses exclusively on purpose-built, standalone solutions. These dedicated solutions are sold directly to enterprises, governments, and telecommunication (telco) and service providers to protect their own infrastructures from attack.

- **Cloud.** Equipment is sold to telcos and cloud providers that in turn build a mitigation services offering that can be sold to enterprises and governments. These services are often cloud based and provide monitoring and mitigation via the providers' security operations center (SOC) and scrubbing centers. Another option IDC has seen is that the service provider will manage the client's on-premise equipment while adding additional management and mitigation from its SOC and scrubbing centers.

- **Hybrid.** The hybrid solution, which a number of end-user organizations are beginning to consider, is a combination of on-premise and cloud defenses. At this stage, these solutions would be better described as defense in depth rather than a true hybrid solution. In this scenario, an on-premise appliance provides defense against smaller volumetric attacks and application layer attacks. The level of visibility and quick response offered by being on-premise is arguably much higher, especially in relation to the application layer traffic. That said, large-scale volumetric attacks can quickly overwhelm an enterprise network. If this occurs, the cloud solution is able to divert the traffic into a scrubbing center before rerouting back to the customer network. The on-premise solution provides valuable information about the attack dynamics that the cloud provider can then use to more efficiently clean the traffic. True joint solutions have not been common, though this may be starting to change. Managed services are offered by some equipment vendors to provide additional resources and intelligence during an attack, but all mitigation is still done on-premise. Cloud providers have been somewhat reluctant to move into the business of selling hardware to this point.

**Service Providers**

For the purposes of this document, IDC uses the term "service providers" to mean providers of cloud services that do not have their own product offering. This includes telcos/carriers, ISPs, and service providers:

- **Akamai:** Kona Security Solutions are part of an overall Web security strategy. Kona Site Defender provides detection, identification, and mitigation of DDoS
and application layer attacks. It is an Akamai-managed service that provides 24 x 7 support with capped bursting fees and no additional charge for DDoS traffic. It provides real-time and historic logging of DDoS traffic events. Natively in path, there is no need for rerouting, no added latency, and no scrubbing. Kona Site Defender leverages the Akamai Intelligent Platform to thwart DDoS attacks by absorbing DDoS traffic targeted at the application layer, deflecting all DDoS traffic targeted at the network layer, such as SYN floods or UDP floods, and authenticating valid traffic at the network edge. Akamai partners with some of the global telcos providing DDoS mitigation.

**FUTURE OUTLOOK**

**Forecast and Assumptions**

The worldwide DDoS prevention products and services market will grow at a CAGR of 18.2% through 2017 and reach $870 million. The product component of the market is expected to grow at 18.8%, while the services component will grow at 17.5%.

Table 1 shows IDC's projected revenue for DDoS prevention products and services for 2011–2017, while Figure 1 is a graphical representation of the market in 2012 and 2017.

The top 3 assumptions and the key forecast assumptions for the worldwide DDoS prevention products and services market are listed in Table 2 and Table 3, respectively.

<table>
<thead>
<tr>
<th>TABLE 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
</tr>
<tr>
<td>Products</td>
</tr>
<tr>
<td>Services</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

Note: See Table 2 for top 3 assumptions and Table 3 for key forecast assumptions.

Source: IDC, March 2013
FIGURE 1

Worldwide DDoS Prevention Products and Services Revenue Share, 2012 and 2017

2012

Services (44.8%)

Products (55.2%)

Total = $376.7M

2017

Services (43.4%)

Products (56.6%)

Total = $869.6M

Source: IDC, March 2013
<table>
<thead>
<tr>
<th>Market Force</th>
<th>IDC Assumption</th>
<th>Significance</th>
<th>Changes to This Assumption That Could Affect Current Forecast</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economy</td>
<td>The global economy will be subdued in 2013, with weak growth in mature economies. Emerging markets will improve, with faster expansion than in 2012, driving worldwide GDP to real growth of 2.6% (on par with last year’s growth). The eurozone will see negative GDP growth, with Southern Europe particularly weak. Japan will also be weak, with post-earthquake reconstruction and stimulus measures having waned, giving way to weak exports and the return of deflation. The U.S. economy is fragile and faces downside risks from political volatility, but we assume that the second half of the year will see some improvement. The good news is that China has recovered its momentum after last year’s slowdown. This in turn will help drive stronger growth in other emerging markets such as India and Brazil. The downside risks are still elevated though, and business confidence will be tepid as a result.</td>
<td>A down economy affects business and consumer confidence, the availability of credit and private investment, and internal funding. A global recession would cause businesses to delay IT upgrades and some new projects; a rising economy does the opposite. A crisis (likely triggered by events in Europe or political wild cards in the United States) could create a level of impact similar to the financial crisis of 2008.</td>
<td>If the worldwide economy slips into a recession, businesses would likely reduce spending and cut security budgets.</td>
<td>This is not IDC’s forecast at this time.</td>
</tr>
<tr>
<td>Market Force</td>
<td>IDC Assumption</td>
<td>Significance</td>
<td>Changes to This Assumption That Could Affect Current Forecast</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Advanced threats</td>
<td>The methods behind DDoS attacks have changed drastically over the course of the past decade. Originally, a DDoS attack was a brute force effort with little focus on stealth or circumventing defenses. As is often the case, as defenses evolved, attackers remained a step ahead and began refining their arsenal to include more stealthy methods such as SYN flood, UDP flood, HTTP GET, and Web application layer attacks in various combinations.</td>
<td>Stealthy attacks that reside in, and look like, legitimate traffic have made the accurate and proactive detection and mitigation of DDoS attacks increasingly difficult. Even more worrisome is the ease with which even low-level cybercriminals can launch a successful campaign against a high-value target. Mitigation solutions that tie in advanced heuristics and intelligence are required to defend against today's attacks and will help drive the market as organizations attempt to keep their defenses ahead of attackers.</td>
<td>If attackers fail to evolve and current technology remains adequate to defend against DDoS attacks, growth may be lower than the current forecast.</td>
<td>Attacks have always evolved and IDC expects this to continue, forcing vendors and service providers to continue to improve their technology, which will drive revenue growth.</td>
</tr>
<tr>
<td>Cloud and mobile infrastructure protection</td>
<td>The expansion of cloud services and mobile networks has created additional targets for DDoS attacks. Hosting companies such as Amazon and Rackspace have a responsibility to their customers to ensure their infrastructure is adequately protected against denial of service attacks. Similarly, with the growth in mobile computing, operators increasingly need to consider DDoS protections when building out their infrastructure.</td>
<td>As hosting providers and mobile operators expand their infrastructure, DDoS protection will be an important component.</td>
<td>If cloud or mobile network growth slows, or is higher than currently forecast, it could cause the DDoS forecast to change.</td>
<td>The current forecasts for mobile and cloud forecast steady growth and are more recession-proof than other markets.</td>
</tr>
</tbody>
</table>

Source: IDC, March 2013
ESSENTIAL GUIDANCE

IDC expects the market for DDoS mitigation solutions to continue to see robust growth. With businesses only becoming more dependent on hosted services and online transactions, protecting infrastructure (whether onsite or offsite) from denial of service attacks will remain a high priority for organizations.

Advice for Providers

Providers of anti-DDoS products and services should continue to expand partnering relationships to address the evolving nature of attacks. At the very least, the coordination and communication between on-premise devices and cloud services should continue to improve, even if the hybrid solution scenario is not formalized. Vendors looking to enter the market would be best served creating a partnership arrangement rather than building a solution from the ground up.

Advice for Users

The capabilities inherent in firewalls, IPS appliances, and other devices may be helpful for very basic attacks or additional intelligence, but in reality, these security devices can become targets themselves because they are unable to recognize seemingly legitimate traffic that is actually part of a flood attack. Dedicated solutions that are able to correlate traffic across sessions and can detect and mitigate application layer attacks are necessary to adequately prevent DDoS attacks. Any organization with a sizable online presence should consider adding dedicated DDoS protection if it has not already. When determining whether to add these capabilities, organizations need to consider not only the actual revenue impact that a loss of service would entail, but the impact on customers and on the brand itself.

Based in part on the business impact determination, as well as resources and budget, the decision on how to implement a prevention solution can be made. Organizations that decide to prioritize DDoS defense would be well served to make it an itemized part of the security budget rather than drawing from another area (such as IPS). When considering an on-premise versus cloud solution, it’s important to recognize that the administrator requirements differ compared with those of a firewall or an IPS solution. For organizations that cannot commit the additional staffing resources, many on-premise providers offer additional managed services to help configure defenses and mitigate attacks in real time. As is often the case, the best solution is often a combination approach where an on-premise appliance and cloud service are used in conjunction when resources allow it.

The truth is that a small percentage of end users utilize a solution crafted specifically to combat DDoS attacks. With the right number of resources effectively trained, such a solution can be very effective. However, with attacks becoming more sophisticated (read: mixed brute force assaults together with targeted application strikes), there is no longer a one-size-fits-all appliance that can outthink attackers on its own.
For those organizations that determine they are most at risk and have made the decision to invest budget in a comprehensive DDoS strategy, IDC finds it should include the following:

- A mix of on-premise and cloud monitoring and mitigation managed internally or externally or a combination of the two
- The ability to handle legacy network attacks and newer, more sophisticated attacks to the application layer and encrypted attacks
- An assessment of the network architecture to determine which parts of the infrastructure (i.e., firewalls and IDP devices/routers) could become a bottleneck during a DDoS attack and which devices have some integrated DDoS capability that could be used in conjunction with dedicated mitigation products and services
- Knowledge and solutions to counter DNS attacks

**LEARN MORE**

**Related Research**


**Methodology**

The IDC market sizing and forecasts are presented in terms of packaged software and appliance revenue. IDC uses the term packaged software to distinguish commercially available software from custom software, not to imply that the software must be shrink-wrapped or otherwise provided via physical media. Packaged software is programs or codesets of any type commercially available through sale, lease, or rental, or as a service. Packaged software revenue typically includes fees for initial and continued right-to-use packaged software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. All of the above are counted by IDC as packaged software revenue. Appliances are defined as a combination of hardware, operating environment, and application software where they are provided as a single package.
Packaged software revenue excludes service revenue derived from training, consulting, and systems integration that is separate (or unbundled) from the right-to-use license but does include the implicit value of the product included in a service that offers software functionality by a different pricing scheme. It is the total product revenue that is further allocated to markets, geographic areas, and operating environments.

The market forecast and analysis methodology incorporates information from five different but interrelated sources, as follows:

- **Reported and observed trends and financial activity.** This study incorporates reported and observed trends and financial activity in 2011 as of the end of September 2012, including reported revenue data for public companies trading on North American stock exchanges (CY 1Q11–2Q12 in nearly all cases).

- **IDC’s Software Census interviews.** IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.

- **Product briefings, press releases, and other publicly available information.** IDC’s software analysts around the world meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.

- **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC also builds detailed information related to private companies through in-depth analyst relationships and maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by product area models on more than 1,000 worldwide vendors.

- **IDC demand-side research.** This includes thousands of interviews with business users of software solutions annually and provides a powerful fifth perspective for assessing competitive performance and market dynamics. IDC’s user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in this study represents IDC’s best estimates based on the above data sources as well as reported and observed activity by vendors and further modeling of data that we believe to be true to fill in any information gaps.

The data in this study is derived from all the above sources and entered into the Software Market Forecaster database, which is then updated on a continuous basis as new information regarding software vendor revenue becomes available. For this reason, the reader should note carefully the “as of” date in the Methodology discussion within the In This Study section, near the beginning of this study.
whenever making comparisons between the data in this study and the data in any other software revenue study.

**Synopsis**

This IDC study examines the DDoS prevention products and services market. It provides a market size for 2011 and 2012 and a forecast for 2013–2017 segmented by products and services.

"With the number of high-profile attacks steadily increasing, the market for DDoS prevention solutions has seen steady growth," said John Grady, research manager for IDC's Security Products program. "IDC believes a defense-in-depth posture with a combination of on-premise equipment and cloud-based mitigation provides the best protection against advanced application and SSL-based attacks as well as large-scale volumetric attacks."

**Copyright Notice**

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2013 IDC. Reproduction is forbidden unless authorized. All rights reserved.