[WHITE PAPER]

The Business Value of DDoS Protection

HOW TO CALCULATE THE ROI FROM A DDoS DEFENSE SOLUTION

ARBOR® NETWORKS

Executive Summary

Today, more and more companies are outsourcing their online operations such as Web sites, ecommerce, email and domain name system (DNS) to focus on core business activities and lower costs. As a result, hosting providers are experiencing double-digit growth as they meet this mounting market demand. Service-level commitments and customer expectations are also on the rise due to the business-critical nature of many hosting services. In particular, the highest-value customers have the lowest tolerance for outages.

A continuing and growing threat to service availability is distributed denial of service (DDoS) attacks. In fact, most hosting providers experience DDoS attacks on a regular basis. An effective DDoS defense system can safeguard business operations against DDoS-related outages, but determining the return on investment (ROI) of purchasing and deploying such a system can be challenging. One needs to quantify both the risks of DDoS attacks and their financial consequences. This paper provides a simple, step-by-step approach for evaluating whether an investment in a DDoS defense system is financially justified.

Using industry averages for attack frequency and outage costs, the results show that investing in an effective DDoS protection solution, such as the Arbor Peakflow® SP Threat Management System ("TMS"), provides a strong positive ROI, reduces customer churn and lowers financial risk. Arbor Networks® also provides an ROI calculator that enables hosting providers to apply their own data to compute ROI and determine the results of different what-if scenarios.

Understanding the Risk of Attack

Few studies focus on the probability that a business will experience a DDoS attack of significant impact. However, survey information from Forrester Research and Arbor Networks provides insight into the risk of such an attack.

Forrester Research conducted a survey of 400 companies with significant online operations.[1] The survey's objective was to gather basic information on the DDoS threat to these businesses, which included online financial services, media, news, political sites, gaming, entertainment, Web hosting and ecommerce. Among the results, over 70% reported at least one DDoS attack in the previous 12-month period. Attack durations were highly variable, but the most common duration for attacks that had operational and business impact was two to six hours.

Arbor Networks' annual *Worldwide Infrastructure Security Report*[2] is an excellent source of more detailed information on the frequency and nature of DDoS attacks on Internet service providers (ISPs) and Internet data centers (IDCs). Based on the responses from 111 ISPs and IDCs, the most recent survey data shows that these organizations are experiencing a high frequency of DDoS attacks—equating to multiple attacks per month (see Figure 1).

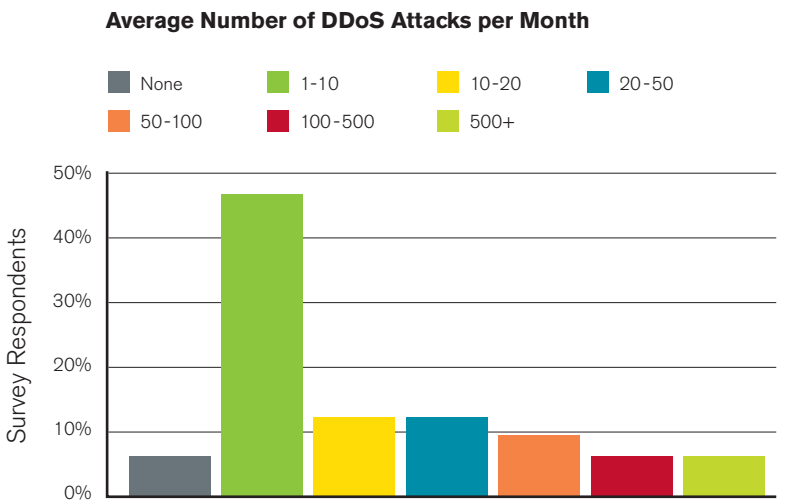

Figure 1
Source: Arbor Networks Annual *Worldwide Infrastructure Security Report,* 2010

McAfee[3] also surveyed IT and security executives from seven industry sectors and found the frequency and impact of DDoS attacks to be similar to those Arbor reported.

In terms of the impact of DDoS attacks, 84% of these ISPs and IDCs reported incurring operational expenses, and 43% reported customer churn and revenue loss (see Figure 2).

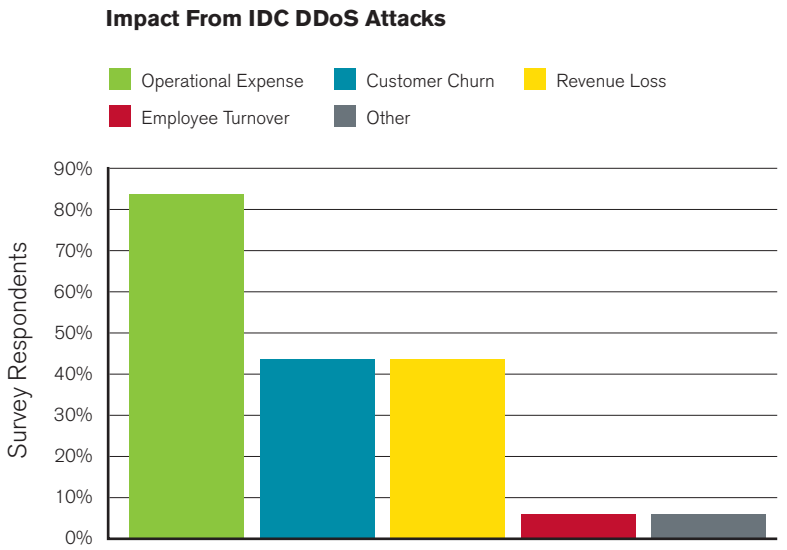

Figure 2
Source: Arbor Networks Annual *Worldwide Infrastructure Security Report,* 2010

Hosting providers in particular often have a higher risk of DDoS attack than stand-alone online businesses because hosting providers in effect aggregate the risk of all their customers. An attack on one customer can affect others and potentially the entire hosting operation because of the heavy reliance on shared infrastructure. Risk is also a function of the type of customers being hosted. Sites that engage in controversial activity, as well as large, visible businesses, are more likely targets of DDoS than small business Web sites. However, just one small customer can attract a massive DDoS response with a single controversial act.

The capacity to unleash a large DDoS attack is available to anyone simply by renting a botnet. Figure 3 shows a typical advertisement for botnet services. Table 1 (see page 4) shows the results of a survey on botnet rental pricing. In short, the resources needed to carry out large-scale DDoS attacks are cheap and readily available.

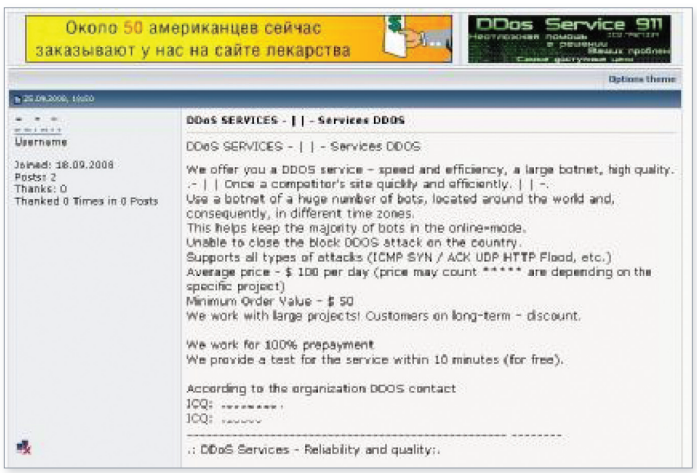

Figure 3: Advertisement for Botnet Services[4]

Price ($)	**Duration** (Hours)	**Bandwidth** (Mbps)
$20	2	45
$30	6	45
$50	12	45
$70	24	45
$75	24	100
$100	24	1,000
$250	24	1,000
$400	5	5,000
$600	168	1,000
$900	24	4,750
$1,000	24	4,750
$5,500	168	4,750
$6,000	168	4,750

Table 1: Botnet Rental Pricing[4]

Botnets are not the only source of DDoS attacks. Social media sites can coordinate large numbers of willing users to carry out DDoS attacks as illustrated by the WikiLeaks-inspired attacks in late 2010. Coordinated through Twitter, large numbers of end users downloaded a simple attack tool and directed attacks at numerous companies deemed complicit in interfering with what the users viewed as the legitimate activities of WikiLeaks. These attacks successfully targeted high-profile companies, including PayPal, MasterCard and Visa. The attacks went both ways as well. The provider hosting WikiLeaks removed the site from its infrastructure because DDoS attacks directed at WikiLeaks were impacting service to all its customers, which in turn might have elicited DDoS attacks from WikiLeaks defenders. This example illustrates the reality that hosting providers bear the aggregated risk of their customers.

The overall impact of a DDoS attack is a function of the time it takes to detect the attack, the time needed to mitigate it and the extent of service degradation both before and after mitigation. For many IDC operators, detection consists of simply waiting for customers to complain, and mitigation consists of dropping all traffic destined to the resource under attack. This form of mitigation may protect the IDC infrastructure and other customers, but it completes the attack on the particular target of the DDoS event. If the target is a high-value customer, the hosting provider will likely suffer financial loss.

Survey data from Arbor,[2] McAfee[3] and Forrester[1] show IDCs are experiencing multiple DDoS attacks per month. Not all attacks result significant outages due to the severity of the attacks themselves and the effectiveness of the anti-DDoS measures deployed at the IDC.

Using the survey data, a conservative estimate of the number of high-impact DDoS events (events resulting in outages of at least 2 hours) is shown in Figure 4. The figure shows the expected number of outages (ranging from 2 hours to over 24 hours) that a typical IDC will experience over a 3-year period. A period of 3 years is used because ROI is generally based on a 3-year time frame.

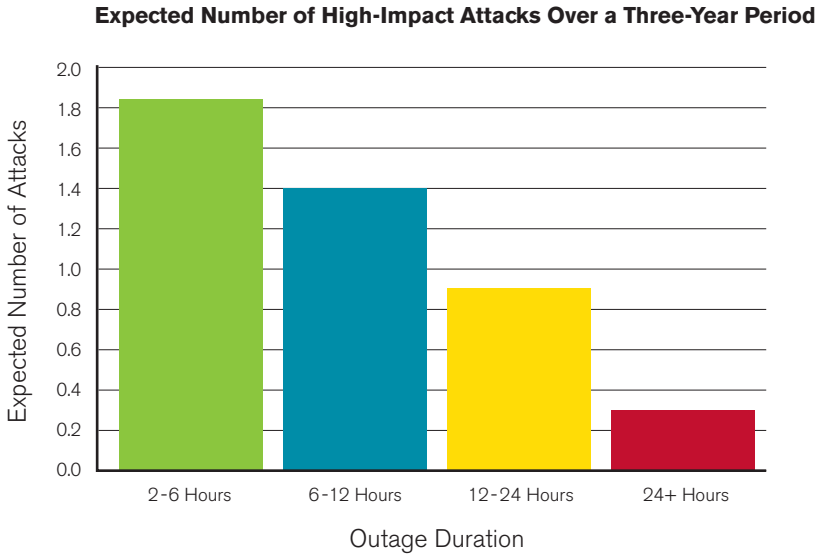

Figure 4

Modeling the Financial Impact of Attacks

The cost of outages due to DDoS attacks is comprised of operational costs and revenue impacts. Lower-impact/duration attacks may only result in added operational costs. High-impact attacks will also negatively affect revenues due to customer defections, SLA credits and reputation damage. The elements contributing to the overall cost of DDoS consist of the following:

- Personnel time spent addressing and recovering from the outage.
- Incremental help desk expenses.
- Customer credits and refunds.
- Cost of customer defections and nonrenewal of contracts.
- Degradation of reputation resulting in higher customer acquisition costs and a lower rate of business growth.

The threshold of DDoS attack likely to result in some or all of these negative consequences varies according to the nature of the business. A good starting point for a hosting provider is to estimate what duration and scope of DDoS attack will have a significant business impact (e.g., customer refunds and credits, customer defections and nonrenewals). Depending on the type of customers served by the provider, the threshold may be an outage ranging from two to six hours to one lasting as long as 24 hours. Lower-level attacks, flash crowds and unanticipated demand can consume engineering and help desk resources but may or may not result in customer defections, credits and reputation loss.

Modeling all of these costs is a good way to determine the benefits of DDoS protection since an effective DDoS protection solution typically reduces these costs by 90% or more. Table 2 provides an example of how organizations can model the total cost per DDoS attack. The example is a hosting provider with $20M in annual sales and an industry-average risk of attack.

Attack Duration (Hours)	**Operations** (# hours x # staff x cost/person/hour)	**Help Desk** (# hours x calls/hour x cost/call)	**Refunds & Credits** (# credits x cost/credit)	**Cancelled, Nonrenewed Contracts** (# nonrenewals x present value of lifetime value of customer)	**Loss of Future Business** (One-year reduction in growth x annual sales)	**Total Cost per Attack**
2-6	4 x 4 x $75	4 x 25 x $20	2 x $800	0	0	$4,800
6-12	9 x 4 x $75	9 x 25 x $20	4 x $800	2 x $20,000	0	$50,400
12-24	18 x 4 x $75	18 x 25 x $20	9 x $800	4 x $20,000	.25% x $20m	$151,600
24+	30 x 4 x $75	30 x 25 x $20	15 x $800	8 x $20,000	.5% x $20m	$296,000

Table 2: Calculating the Total Cost of Each DDoS Attack

Combining the DDoS attack risk profile with attack cost estimates produces the expected cost over three years, as shown in Table 3.

Attack Duration (Hours)	**Expected Number of Attacks Over 3 Years**	**Cost per Attack**	**Expected Cost Over 3 Years**
2-6	1.9	$4,800	$9,120
6-12	1.4	$50,400	$70,560
12-24	0.9	$151,600	$136,440
24+	0.3	$296,000	$88,800
TOTAL EXPECTED COST			**$304,920**

Table 3: Three-Year Expected Cost of DDoS Attacks

This cost can now be compared to the alternative of investing in a high-quality DDoS defense system, which can be expected to eliminate the extraordinary expenses of dealing with DDoS attacks through traditional methods (e.g., black-holing customer traffic, removing domains, etc.). The cost of an effective DDoS protection system is generally a function of mitigation capacity—that is, how much attack traffic the device can handle. This example assumes that a system capable of mitigating 2.5 Gbps is sufficient and can be purchased for $100K. Annual ongoing ownership costs (e.g., support, maintenance, internal operations, etc.) are about 25% of the purchase price.

There is also a positive revenue component to investing in DDoS protection. DDoS was ranked the number-one network security issue in a survey of 400 IT professionals by Forrester Research. Therefore, as high-value customers make decisions on obtaining data center hosting services, the ability of a hosting provider to address this key concern will influence the purchase decision.

The result is, other factors being equal, a hosting provider that includes DDoS protection as part of its standard service will likely attract more new business than a hosting provider that does not. This incremental revenue should be included in the ROI calculation. A conservative estimate is .25% incremental growth over what would be achieved without DDoS protection in the standard offering. For example, a hosting provider expecting 12% growth would increase forecasted growth to 12.25%. Thus, a hosting provider with $20M in annual sales would derive $50K in incremental revenue per year as a result of being able to protect customers from outages due to DDoS. The three-year present value (PV) at 10% discount rate of the incremental revenue for just one year of additional growth is approximately $124K.

Using the data above, Table 4 shows the final results of the three-year net present value (NPV) and ROI of the investment (not including residual value of the equipment).

	ROI
Initial Investment	$100,000
Year 1 Return—Ownership Costs	$127,000
Year 2 Return—Ownership Costs	$127,000
Year 3 Return—Ownership Costs	$127,000
NPV (@10% Discount Rate)	$196,000
ROI	281%
Payback	9.4 Months

Table 4: NPV and ROI of a DDoS Defense Solution

Choice of the DDoS protection solution matters. As explained in the Arbor Networks' white paper entitled *The Growing Need for Intelligent DDoS Mitigation Systems,* traditional perimeter security products such as firewalls and intrusion prevention systems (IPS) are unable to address the DDoS threat to availability. To realize the projected benefits of deploying a DDoS defense solution, due diligence is needed on the part of the technical staff when selecting a solution.

Using the Model

A hosting provider using this model to project the ROI of a DDoS defense solution must of course adjust the inputs based on its own experience of DDoS attacks, operational costs and business impact. The accuracy of the estimate depends in part on how well the provider understands the effects of prolonged outages and damaged reputation on customer buying behavior. The highest-paying and highest-value customers are most affected by outages and service degradation, so it is important to be sensitive to downtime costs from a customer perspective. Data from the *Symantec 2011 SMB Disaster Preparedness Survey*[5] shows the median cost of downtime for small-to-medium businesses is $12,500 per day. Thus, the aggregate cost of a major outage affecting 100 customers is approximately $1.25M and could well result in significant defections as customers rightly conclude that availability is critical to their bottom line.

Lastly, in addition to modeling the best estimate of ROI, it is also useful to model the upside and downside risks of making the investment. Figure 6 shows the break-even point and financial sensitivity for protecting against the risk of major attacks that result in extended outages (24+ hours). This is a cost-only view and does not include any incremental revenue growth from offering DDoS protection. Figure 5 graphs the three-year cost of extended outages with respect to frequency of attack. The financial break-even point in this case is a frequency of one major outage every six to seven years. Also significant is the difference between the upside and downside risk. The graph shows that the cost of not being able to effectively address DDoS attacks rises very steeply as frequency goes up; thus, the cost exposure of underestimating attack frequency is very high. In contrast, if the actual frequency is less than expected, the cost exposure of having overinvested in DDoS protection is gradual and bounded by the amount invested. Finally, the graph illustrates how the investment in DDoS protection replaces a highly uncertain and steep cost curve with a flat, predictable and relatively low cost curve. This is clearly a more desirable operating model for financial managers.

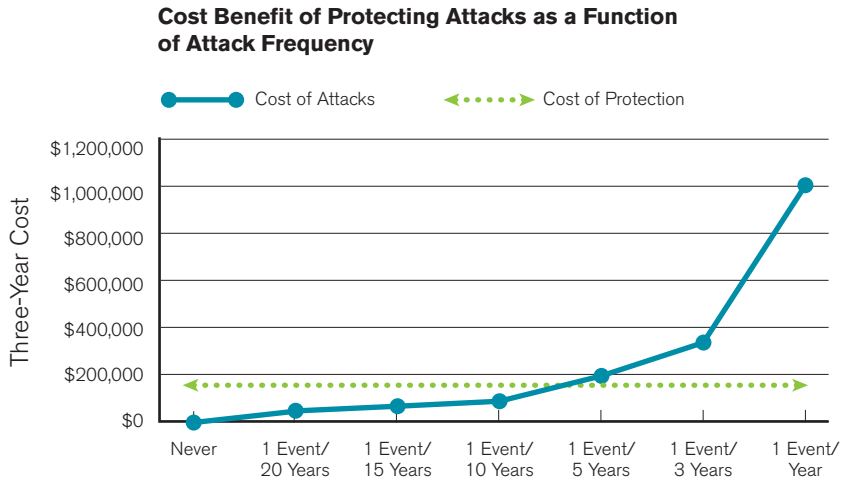

Figure 5

ROI Calculator for DDoS Protection

The method shown previously is relatively easy to apply to a hosting operation. Arbor Networks also provides an ROI calculator based on this method. The calculator provides default values that make it easy to get an initial estimate and also lets users enter values that more accurately reflect the realities of their own operations. The user can try plugging in different values to test the sensitivity of the results to changes in various inputs. The user is asked to provide the following information:

Required Inputs	Comments
Average number of business-impacting DDoS events per year (2-6 hours)	Industry average is .8 per year
Man-hours of network engineering time per hour of DDoS attack or outage	Default of 4 man-hours provided—appropriate for small- to mid-sized hosting data centers
Network engineering personnel cost per hour	Average fully loaded cost is $75 per hour
Number of help desk calls per hour of outage	
Cost per help desk call	Industry average for Tier 1 help desk is $20 per call
Average $ value of SLA credit per customer if credits are issued	Typically 1 month of billing per credit
Number of customer credits issued per 8 hours of outage	
Number of lost customers per 8 hours of outage (nonrenewals)	
Annual revenue per customer	
Average customer retention time (years)	
Percent business growth impact (negative) after serious outage (18 hour plus)	Suggested value is .25% (reputational damage)
Percent business growth impact (positive) if DDoS protection is added to standard offering	Suggested value is .25%
Annual company revenue	
Bandwidth requiring DDoS protection (Gbps)	

Table 5: ROI Calculator Required Inputs and Default Values

Conclusion

Today's hosting provider can increase revenue by capitalizing on the growing demand of business customers for hosted online operations—provided, of course, that it can safeguard these critical operations against DDoS-related outages. To minimize such outages and optimize the availability of their hosting services, providers are turning to DDoS defense solutions such as the Arbor Peakflow SP Threat Management System. Faced with budget constraints, however, they must first evaluate whether an investment in a DDoS protection solution is financially justified. Using the simple, step-by-step approach described in this paper, providers can model the financial impact of a DDoS attack on their operations and calculate the ROI of an effective DDoS defense solution.

Visit www.arbornetworks.com for more information.

References

1 *The Trends and Changing Landscape of DDoS Threats and Protection,* Forrester Consulting, July 2009.

2 *Worldwide Infrastructure Security Report,* Arbor Networks, January 2010.

3 *In the Crossfire: Critical Infrastructure in the Age of Cyber War,* Authors: Stewart Baker, distinguished visiting fellow at CSIS and partner at Steptoe & Johnson; Shaun Waterman, writer and researcher, CSIS; George Ivanov, researcher, CSIS; McAfee, 2010.

4 *Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study,* Vicente Segura and Javier Lahuerta, Department of Network and Services Security, Telefonica I+D.

5 *Symantec 2011 SMB Disaster Preparedness Survey,* Symantec, 2011.

Corporate Headquarters

6 Omni Way
Chelmsford, Massachusetts 01824

Toll Free USA +1 866 212 7267
T +1 978 703 6600
F +1 978 250 1905

Europe

T +44 208 622 3108

Asia Pacific

T +65 6299 0695

www.arbornetworks.com

WP/BVDDoSP/0211

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for converged carrier networks and next-generation data centers, including more than 70 percent of the world's Internet service providers and many of the largest enterprise networks in use today. Arbor's proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the Active Threat Level Analysis System (ATLAS®). Representing a unique collaborative effort with 100+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.