Forrester Consulting
MAKING LEADERS SUCCESSFUL EVERY DAY

FORRESTER®

July 6, 2009

The Trends And Changing Landscape Of DDoS Threats And Protection

Why You May Need To Consider Alternative DDoS Protection

A commissioned study conducted by Forrester Consulting on behalf of VeriSign, Inc.

FORRESTER®
Headquarters
Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • www.forrester.com

Table Of Contents

Executive Summary

In March 2009, VeriSign commissioned Forrester Consulting to conduct a study on distributed denial of services (DDoS) threats and protection. This survey included 400 respondents from the US and Europe and was designed to provide quantitative data regarding today's DDoS threats and companies' defense strategies against these threats. Our goal is to paint an accurate picture of the state of preparedness against ongoing DDoS threats and provide concrete information regarding available defenses for IT decision-makers who face DDoS attacks in their day-to-day operations.

The study uncovered these key findings:

- **DDoS is a top-of-mind concern for security professionals.** Our respondents chose "Defending against DDoS" as the top time-consuming IT security threat. In addition, the majority of respondents indicate that they are "concerned" about DDoS and are actively investigating protection measures.

- **DDoS attacks are a common occurrence.** Nearly 75 percent of respondents have seen one or more DDoS attacks in the past 12 months. Targeted attacks are prominent.

- **ISPs often fall victim to DDoS attacks.** Our survey respondents expressed concerns over their ISPs' viability to combat DDoS attacks. More than half of those we surveyed reported that they saw their ISPs' services disrupted by DDoS attacks in the past 12 months.

- **Current anti-DDoS measures are not sufficient.** Concrete attack and recovery time statistics point to the fact that current DDoS protection measures failed to quell DDoS threats. Many have experienced service disruption due to DDoS.

- **The industry, as a whole, is not ready for large-scale DDoS attacks.** While small attacks can be detected and blocked by the various means of anti-DDoS measures, our respondents expressed serious doubt as to the industry's ability to withstand large-scale attacks.

We found that a wide range of anti-DDoS mechanisms were in use in the survey respondents' organizations, including on-premise detection/prevention, ISP anti-DDoS services, third-party anti-DDoS services, and bandwidth over-provisioning. Only an extremely small percentage of companies we surveyed have not yet provisioned any capability to guard against DDoS. Despite all this, we found that DDoS remains a prevalent threat and that most companies are ill prepared to deal with massive-scale DDoS attacks.

It is therefore Forrester's opinion that current DDoS protection technologies are not sufficient against large-scale attacks. Organizations that are concerned about DDoS should seek alternative methods for DDoS detection and prevention. More specifically, they should seek technologies and services that have enough capacity to deal with massive-scale traffic, respond quickly before attack traffic saturates the victim network, and which are agile enough to quickly provision defenses.

Survey Methodology And Respondent Demographics

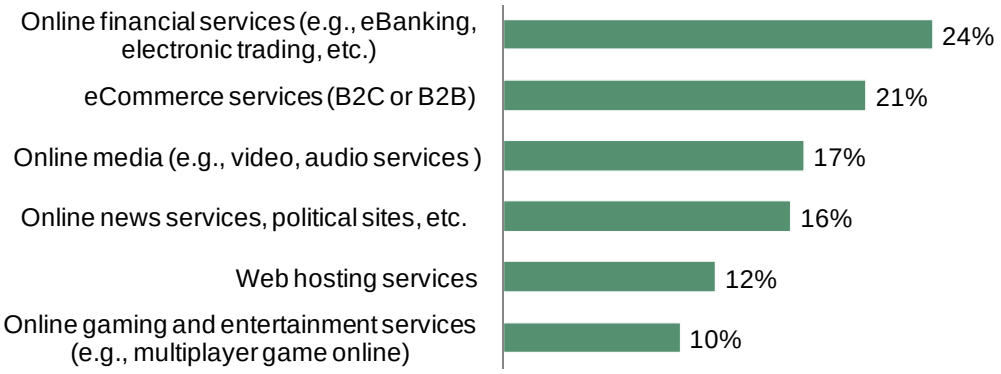
The survey study included 400 participants, all IT decision-makers, from US and EMEA regions. To help focus the study, the participants were from companies that either operate a significant online business or enjoy an important online reputation. More specifically, our survey included these industry verticals:

- Online financial services.
- Online media.
- Online news and political sites.
- Online gaming and entertainment services.
- Web hosting services.
- eCommerce services.

The specific industry distribution of the survey respondents is shown in Figure 1.

Figure 1: Industry Distribution Of Survey Respondents

"Which of the following most closely describes your company's online business?"



Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

A specific qualifying criterion for the survey respondents is that their organizations must have at least one of the following characteristics:

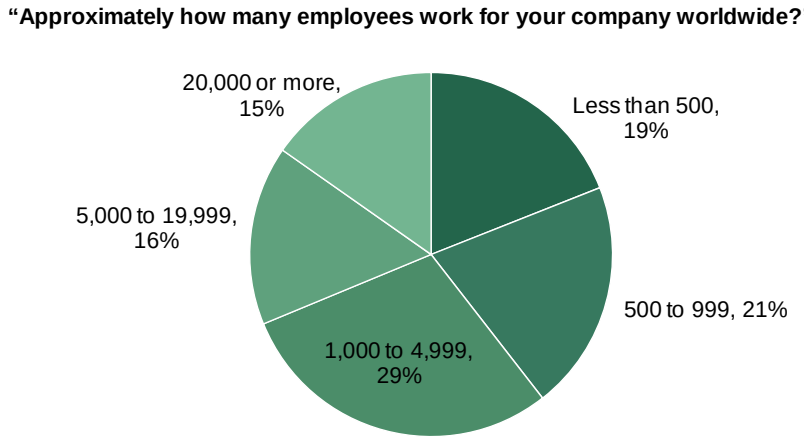
- Require 24x7 access to their online services.
- Have important online reputations.
- Receive significant revenue from their online services, and disruption would cause serious financial loss.

The survey itself contained 25 content questions and 10 screening questions, all multiple choice. The questions spanned topics such as outlook on DDoS attack trends, actual experiences of attacks, organizational processes for incident response, and technologies used to protect the corporate network. To make things simple, we used minimal branching logic in the survey questions.

Of the 400 survey participants, 200 were from the US and the rest from across EMEA regions, including the United Kingdom, Germany, and France. All respondents were directly involved in network operations or network security. Their roles include senior IT manager, director of IT, director of operations, network security manager, and network architect, all with direct responsibility in response to network attacks like DDoS.

The organizations represented in this survey range from SMBs with fewer than 500 employees to enterprises with 20,000 or more workers. The distribution of company size is shown in Figure 2.

Figure 2: Organization Size Distribution



Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

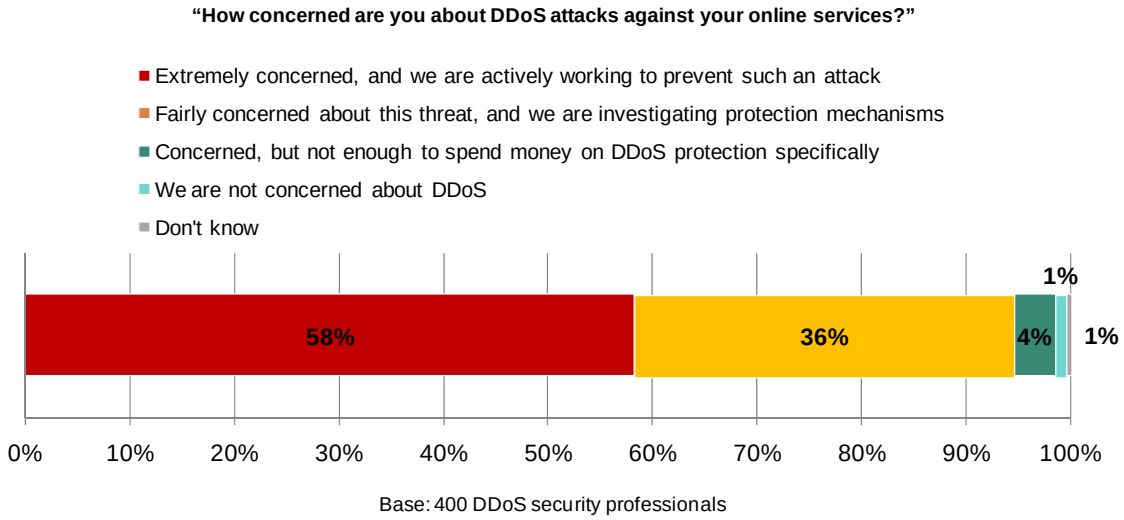
All the data and analysis results used in this study are presented in an aggregate and anonymous form and are used with the permission of survey respondents. We should note that this study is specifically aimed at distributed denial-of-service threats, which differ from denial-of-service (DoS). While a DDoS attack necessarily involves multiple attack sources and the attack traffic is typically distributed across many segments of the Internet, a DoS attack can come from one or a very small number of concentrated sources. As DDoS attacks are the main focus of this study, the findings contained in this survey pertain only to risks associated with DDoS, not to other network security issues.

DDoS Is A Top-Of-Mind IT Concern

Many of our survey participants told us that DDoS was a top-of-mind threat to their online services. When asked how concerned they were about DDoS attacks, 58 percent indicated they were *extremely* concerned about DDoS and were actively working to prevent such attacks. Another 36

percent said they were fairly concerned and investigating DDoS protection mechanisms (see Figure 3).

Figure 3: Concerns over DDoS attacks



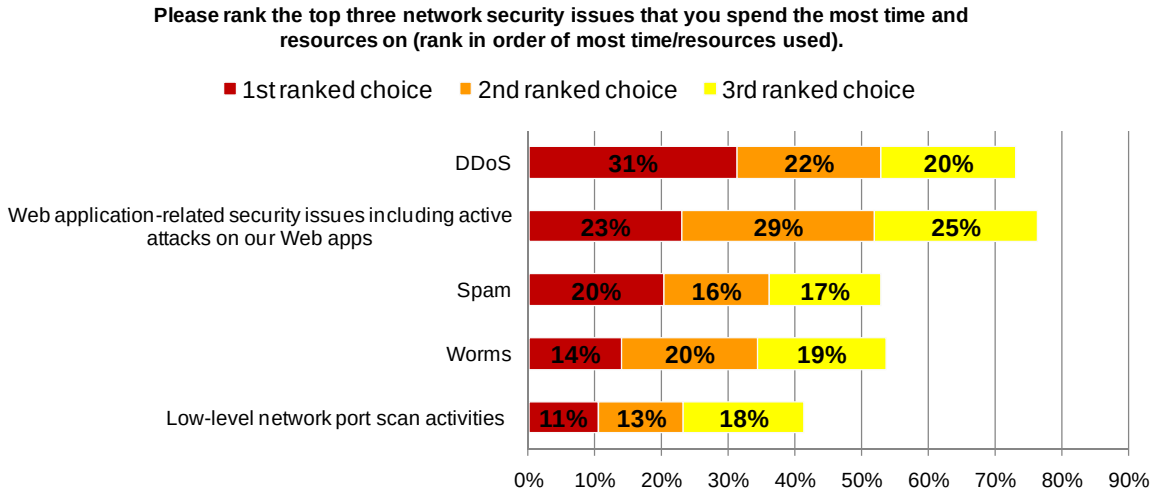
Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

It is no surprise that DDoS was considered a significant threat. As later statistics in the study will show, 74 percent of survey respondents reported that their organizations had been the target of one or more DDoS attacks in the past year.

In addition, when we asked the respondents to rank the top three network security issues on which they spend the most time and resources, dealing with DDoS attacks was the top-ranked issue, followed by Web application security issues and spam (see Figure 4) .

Figure 4: Top Three Security Issues Taking Up The Most Time And Resources



Base: 400 DDoS security professionals

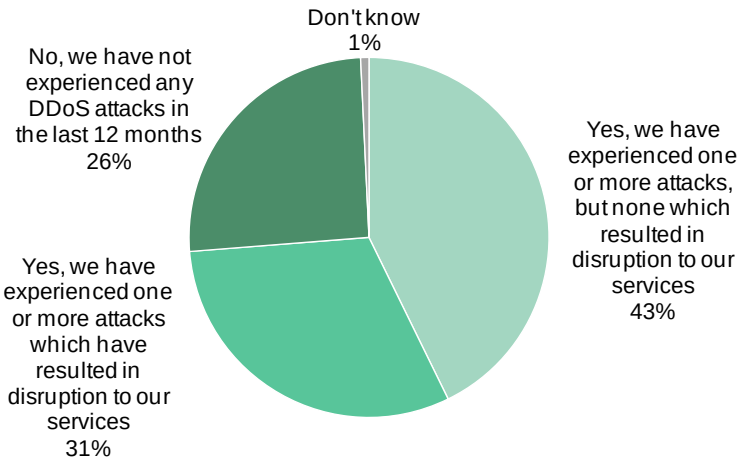
Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

DDoS Attacks Are Rampant

To understand how prevalent a threat DDoS is, we asked respondents whether their organizations experienced any DDoS attacks in the past 12 months. Alarmingly, 74 percent reported seeing one or more DDoS attacks. Of these, 31 percent said the attacks resulted in service disruption, while another 43 percent reported seeing attacks that did not disrupt their services (see Figure 5).

Figure 5: DDoS attack experiences

"Has your organization experienced any DDoS attacks in the past 12 months?"



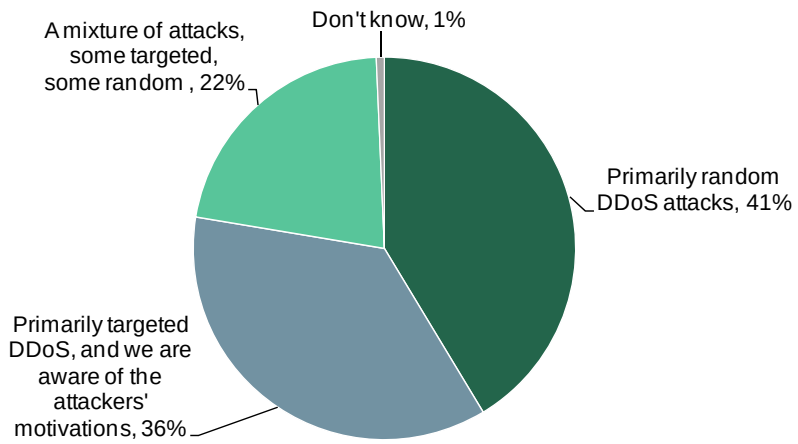
Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

It is worth noting that targeted DDoS attacks surfaced prominently in our survey. In a targeted DDoS attack, all attack traffic is directed specifically to the victim—typically no one else is affected. These attacks often involve application-level tactics that are purposely designed to target the victim's services. In contrast, a random attack may target multiple or even a large number of victims, and they often involve only network-level attacks. A targeted attack is often staged by someone (or some organization) who wants to do harm specifically to the victim. Of those respondents who experienced DDoS attacks, nearly half were targeted attacks as opposed to random ones — 36 percent of those who had seen DDoS attacks reported they were primarily targeted attacks, while 41 percent reported seeing only random attacks. The remaining 22 percent reported a mixture of targeted and random attacks (see Figure 6).

Figure 6: Types Of Attacks Experienced

"Which of the following best describes the type of attacks your organization has experienced in the past 12 months?"



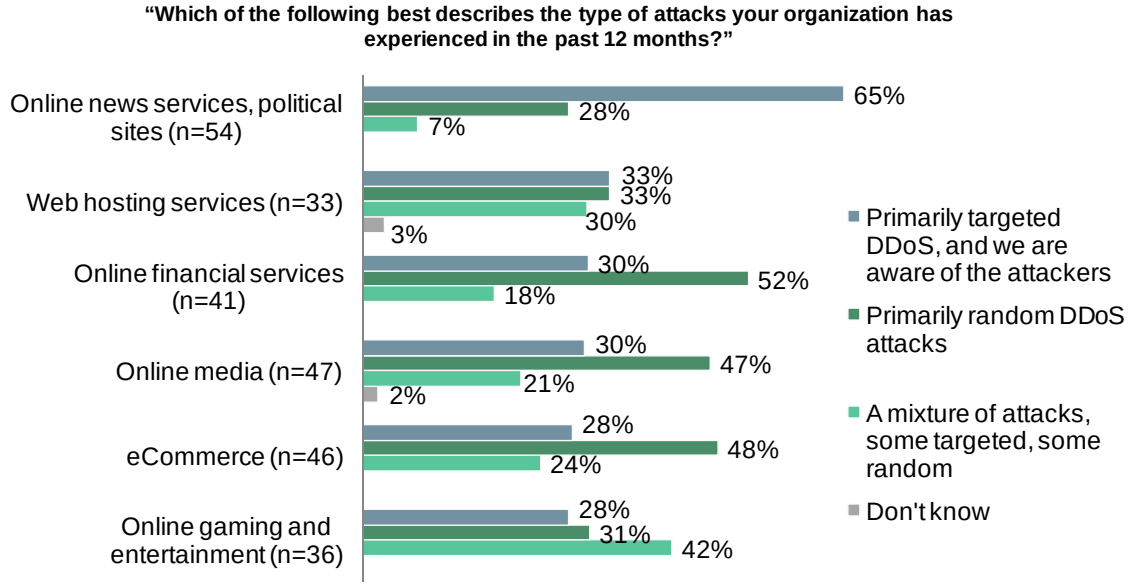
Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

Looking across the different industries, it is clear that whether an organization sees more targeted versus random attacks has much to do with the business itself. Figure 7 depicts the breakdown of targeted and random attacks seen by respondents from different industries. As shown, online news/political sites saw substantially more targeted attacks than random ones. Web hosting and online gaming companies experienced equal amounts of targeted and random attacks, while eCommerce, online financial services, and online media companies saw primarily random attacks.

As the ways to conduct business on the Internet evolve, so are the methods of online attacks. Three to five years ago, DDoS attacks were primarily random attacks (e.g., SYN floods). Today, we are seeing more and more targeted attacks, suggesting the motivation and tactics behind attacks are changing. Targeted attacks are often harder to detect than random ones because they may intentionally mimic legitimate application traffic. This troubling trend points to the need for new attack detection and prevention methods — the traditional ways of threshold-based detection aren't likely to work in the face of the newer, more insidious targeted attacks.

Figure 7: Online News And Political Sites Experience Highest Rate Of Targeted Attacks



Base: DDoS security professionals from organizations with each type of online business who have experienced at least one DDoS attack in the past 12 months

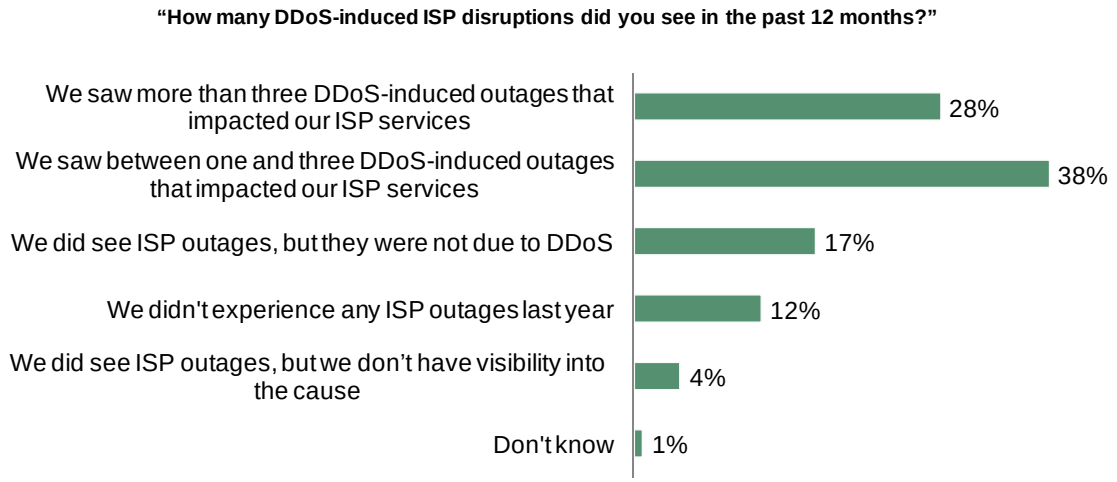
Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

It is not surprising that online news/political sites would attract more targeted attacks than other industries. After all, political sites have long been the target of concerted attacks, with or without the means of DDoS.

Many Saw Their ISPs Fall Victim To DDoS Attacks

Of the companies surveyed, 62 percent reported that they were using DDoS protection services offered by their ISPs. At same time, however, ISPs are often themselves the target of DDoS attacks. Some 66 percent of our respondents reported that they saw at least one DDoS-induced ISP outage in the past 12 months, with 28 percent reporting more than three ISP outages due to DDoS attacks (see Figure 8).

Figure 8: DDoS Induced ISP Outages



Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

Today, many second-tier ISPs' bandwidth connections to their upstream providers are somewhere in the neighborhood of 10GB/sec. With the largest DDoS attacks now reaching nearly 40GB/sec, it is no surprise that some ISPs would be susceptible to DDoS attacks.

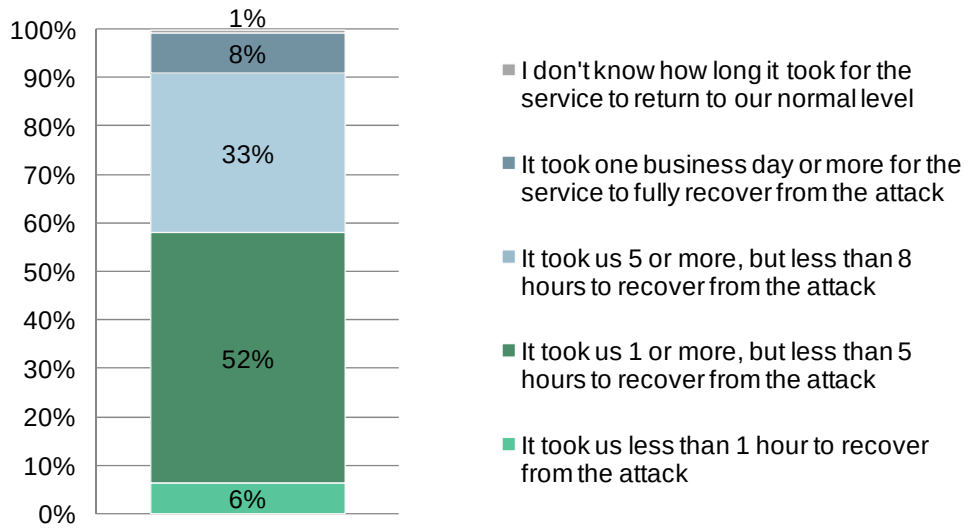
For those that rely on the availability of their Internet connectivity and/or the ability of their ISP to offer DDoS protection, multiple ISP outages per year are simply not acceptable. If a DDoS attack takes down an ISP, it would by definition take down their DDoS protection service.

Recovering From A DDoS Attack Requires Significant Resources

A total of 124 survey respondents said their organizations experienced one or more DDoS attacks that disrupted their services. For those 124 IT decision-makers, recovering from the effects of the attack was a non-trivial undertaking: 64 reported that it took them between 1 and 5 hours to restore their services, while 41 said the recovery process took between 5 and 8 hours. A smaller percentage,10 respondents, indicated that it took more than one business day to fully restore their services (see Figure 9).

Figure 9: Recovering Time From A DDoS Attack

"How long did it take your organization to recover from the most severe DDoS attack you have experienced?"



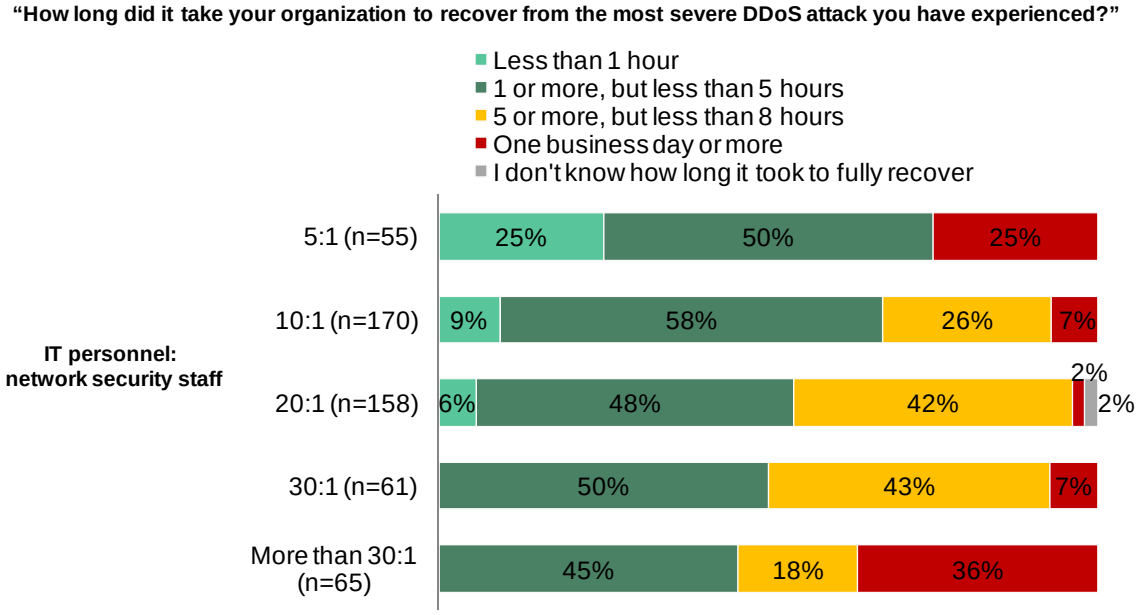
Base: 124 respondents who experienced a DDoS attack that disrupted services

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

In a previous VeriSign-commissioned Forrester study, we interviewed 18 large organizations whose online presence is core to their business. For those organizations, a disruption in their online services would result in a significant loss of revenue, even if the disruption was only for a short duration. In fact, it is not uncommon for an organization to lose millions of dollars per hour when service is down.[1]

Interestingly, we observed that the recovery time from a successful DDoS attack is largely proportional to the percentage of security staff in IT. In our study, 25 percent of those who boast a 1 to 5 security/IT staff ratio said it took less than 1 hour to recover from an attack. In contrast, only 9 percent of those with a 1 to 10 security/IT ratio were able to restore their services within an hour, and that number dropped to 6 percent for those with a 1 to 20 security/IT ratio (see Figure 10).

Figure 10: Higher Ratios Of Dedicated Network Security Staff Show Decreased Recovery Time From DDoS Attacks



Base: DDoS security professionals reporting each ratio of IT personnel to dedicated network security staff

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

These data points suggest that defense against DDoS and speedy recovery from a successful attack requires significant security expertise. In today's economic climate, where many organizations are looking to reduce headcount and resource spending, a sizable internal security staff may be a rare occurrence or simply unattainable. It is therefore all the more important that successful DDoS detection and prevention is executed before the attack causes damage.

Organizational Response To DDoS

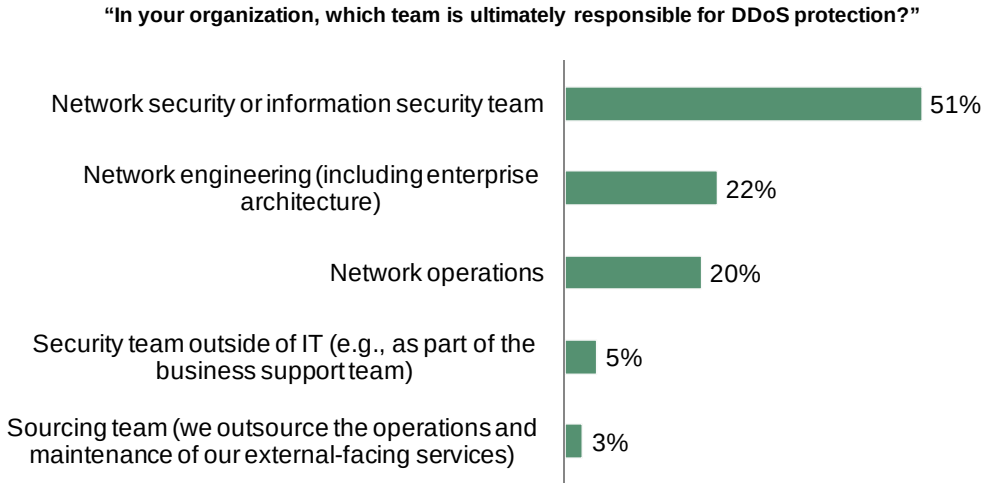
Respondents were asked how their organizations deal with DDoS threats today. Two key trends stood out among the survey responses:

- The network security team is primarily responsible for defense against DDoS.
- The network security team represents a small fraction of the organization's IT staff.

We asked our respondents which team in their organization is responsible for DDoS protection. More than 50 percent said their network and information security team is responsible for DDoS protection, followed by network engineering and operations teams at 22 percent and 20 percent, respectively. The detailed responses are summarized in Figure 11.

As alluded to previously, we also asked our respondents the ratio of their security staff to IT staff in general. The answers we received indicate that most companies have a 1 to 10 or 1 to 20 security to IT staff ratio (see Figure 12).

Figure 11: Who Is Responsible For DDoS Protection In Your Organization?

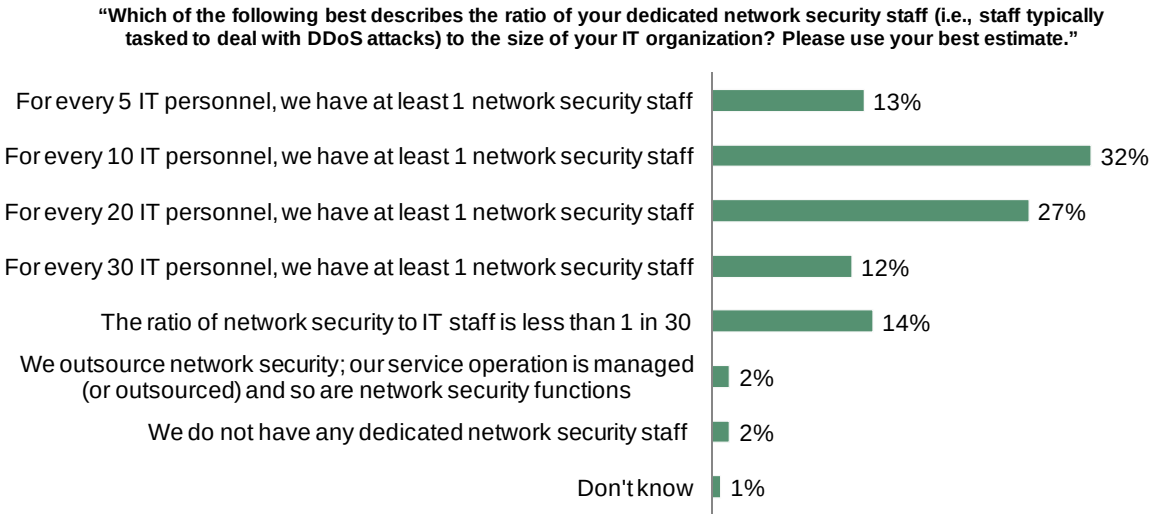


Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

The security to IT staff ratio is interesting because it tells us how prominent a role security plays in an internal IT strategy. As we noted earlier, the recovery time from a successful DDoS attack appears to be proportional to the percentage of security staff within IT (see Figure 10). The statistics suggest that for those with a 1 to 30 or less security to IT ratio, responding to and recovering from a successful DDoS attack often involves a prolonged process, which can be costly to the business.

Figure 12: Ratio Of Security To IT Staff



Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

Current Anti-DDoS Methods Do Not Provide Sufficient Protection

Our study revealed that today almost every organization is using some form of DDoS protection. Only 1 percent of the respondents, a total of four organizations, reported that their companies are not using anything to prevent DDoS attacks. The available DDoS protection means typically include the following:

- **On-premise detection and protection.** This functionality typically operates at the edge of a corporate network, attempting to decipher whether incoming traffic constitutes DDoS attack traffic. The detection method usually involves threshold-counting, behavior pattern detection, etc. Once an attack is detected, a new firewall access control list or a traffic throttling mechanism may be established to drop and control traffic coming from certain attack sources.

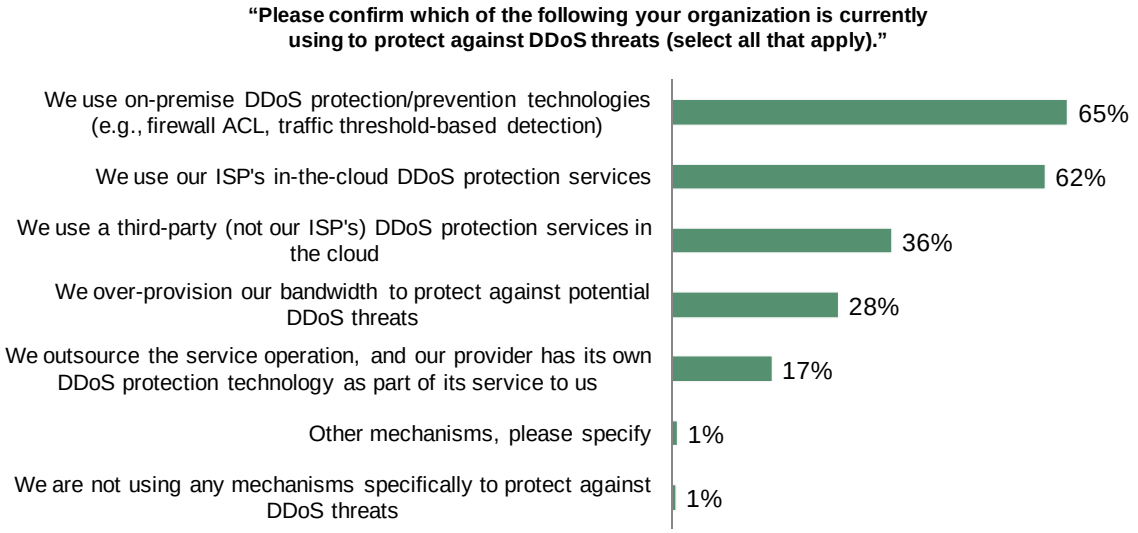
- **In-the-cloud DDoS protection by an ISP.** Many ISPs offer this type of service, whereby the ISP attempts to filter out attack traffic targeting a specific customer. An ISP-based DDoS protection method can drop attack traffic before it hits the edge of the victim network, which alleviates resource burdens required for an on-premise DDoS protection solution.

- **Third-party (not your ISP) offered in-the-cloud DDoS protection.** This method is similar to those offered by an ISP, except that the traffic is routed to a non-ISP data center to be processed for potential DDoS attacks. An added benefit of a third-party DDoS protection is that, unlike an ISP whose primary business is routing traffic, this third-party can specialize in DDoS attack detection and prevention, which means it could respond more quickly than an ISP or have more capacity to deal with attacks. Further more, a third-party DDoS protection service can be carrier (ISP) agnostic, and therefore less likely to be affected by a carrier-specific issue.

- **Bandwidth over-provisioning.** Some organizations opt to over-provision their available bandwidth to absorb DDoS attack traffic. In an earlier Forrester study, also commissioned by VeriSign, we found that many large organizations chose this method to allow for peak traffic as well as attack prevention.[2]

Figure 13 details the various attack detection/prevention mechanisms used by our respondents.

Figure 13: Current DDoS Protection Mechanism Used



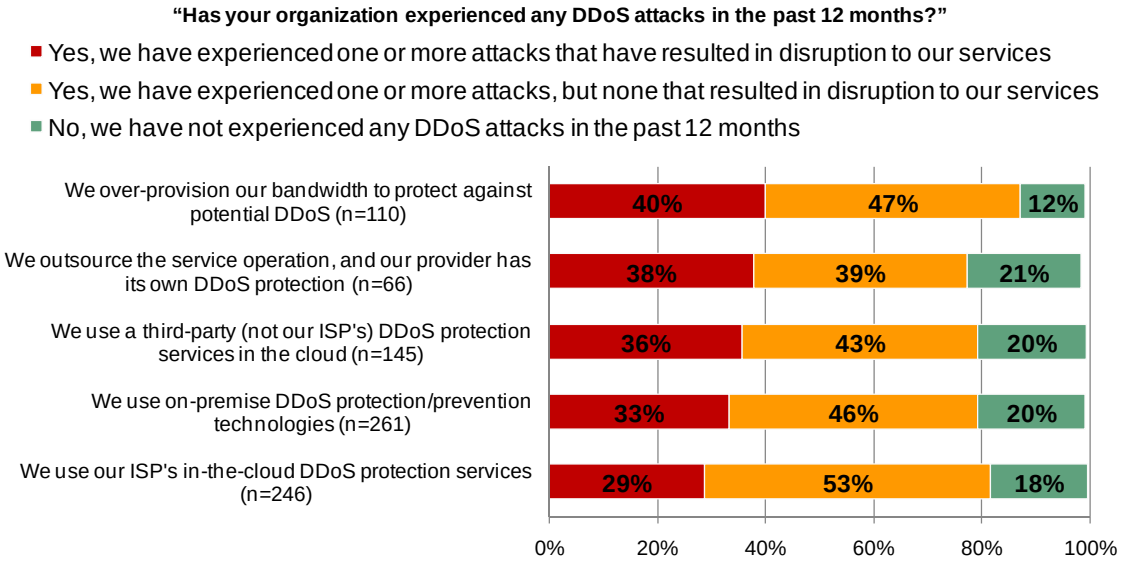
Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

As shown, on-premise DDoS protection/prevention technologies, such as firewall access control list and traffic throttling, are the number one choice among our respondents. Using an ISP's in-the-cloud DDoS protection service was a close second, followed by third-party protection services and bandwidth over-provisioning.

To gain some perspective into the effectiveness of the various solutions, we looked into how each technology fared against DDoS attacks reported by our respondents. The results are depicted in Figure 14.

Figure 14: Successful DDoS Attacks By Protection Method



Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

Forty percent of respondents who over-provision bandwidth to defend against DDoS attacks saw their protection mechanism fail and service disrupted. Similarly, 36 percent of those using third-party DDoS protection services experienced service-crippling attacks. Thirty-three percent of on-premise anti-DDoS technology users saw successful DDoS attacks against their organization, and 29 percent of those using their ISPs' DDoS protection services fell victim to DDoS attacks.

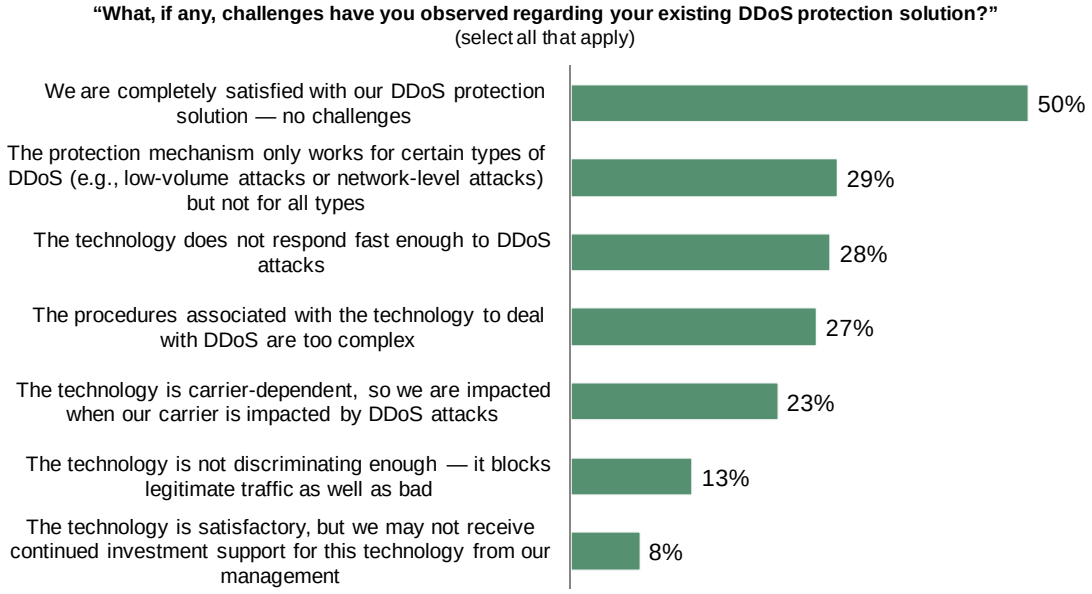
These data tell us that today's DDoS protection mechanisms, in their various forms and modes, are far from perfect. None offered impenetrable or even good enough protection against DDoS attacks. Of these, bandwidth over-provisioning is the least effective.

Our respondents helped to shed a bit more light on why some of them felt the current protection mechanisms are less than effective, when asked to detail their specific challenges with the existing anti-DDoS solutions. The answers singled out three top challenges:

- The protection mechanism only works for certain types of attacks.
- The technology does not respond fast enough to attacks.
- The procedures associated with the technology are too complex.

Figure 15 summarizes the detailed answers. As shown, 29 percent of respondents felt that the protection mechanism only works for low-volume or network-level attacks and are less effective for other attack types. Twenty-eight percent indicated that their DDoS protection did not respond fast enough to attacks, while 27 percent thought the technology and associated procedures were too complex. The other 23 percent expressed concerns over the technology being carrier-dependent.

Figure 15: Challenges With Existing DDoS Protection Mechanisms

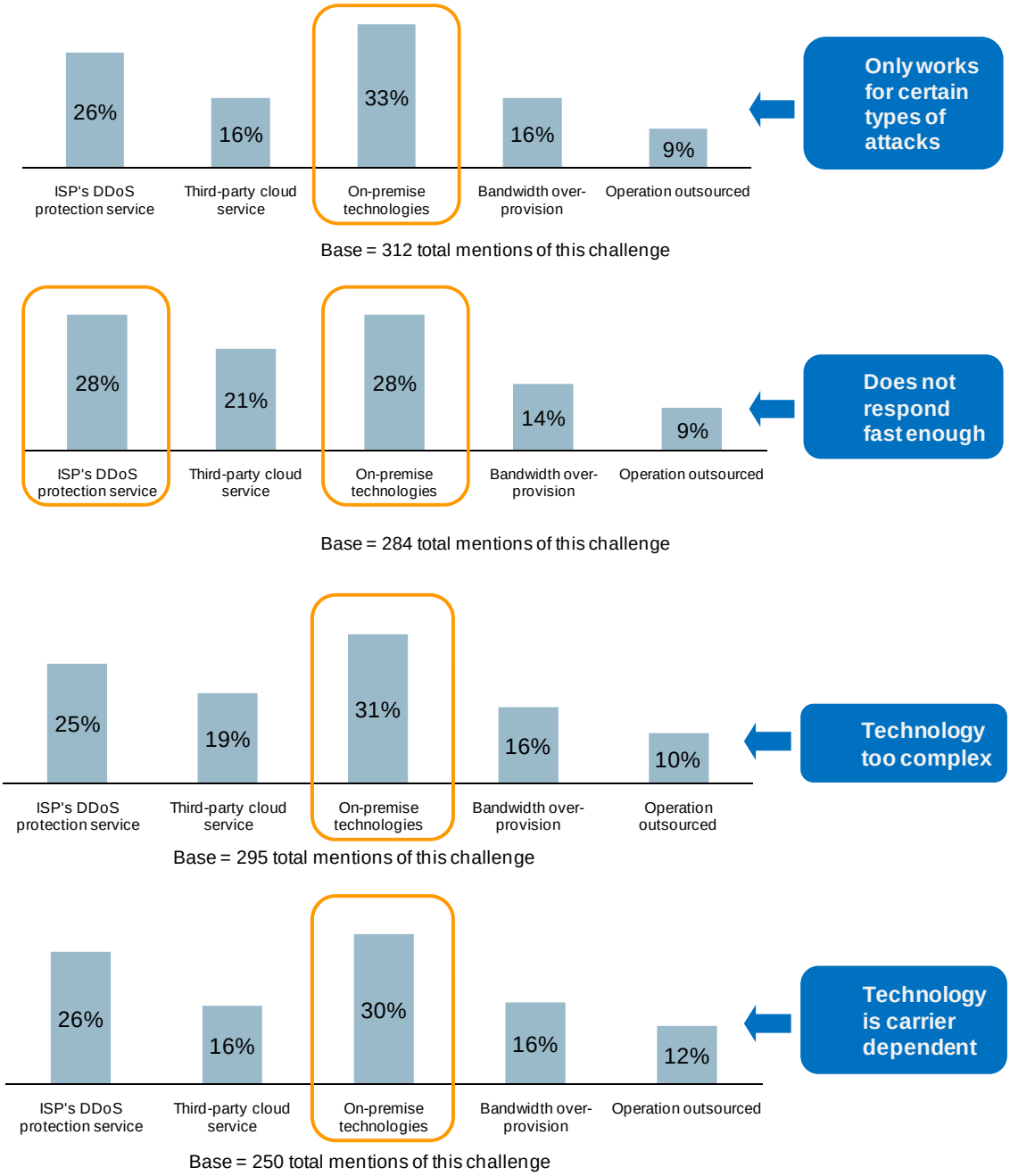


Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

A deeper look at the data suggests that more people using ISPs' DDoS protection services and on-premise technologies complained that the technology did not respond fast enough to attacks (see Figure 16). More people using on-premise technologies expressed concerns over the complexity of the technology and that it only works for certain types of attacks. Those who complained about the carrier-dependent nature of the technology were primarily using on-premise and ISP DDoS protection technologies.

Figure 16: Challenges With Existing DDoS Protection Mechanisms



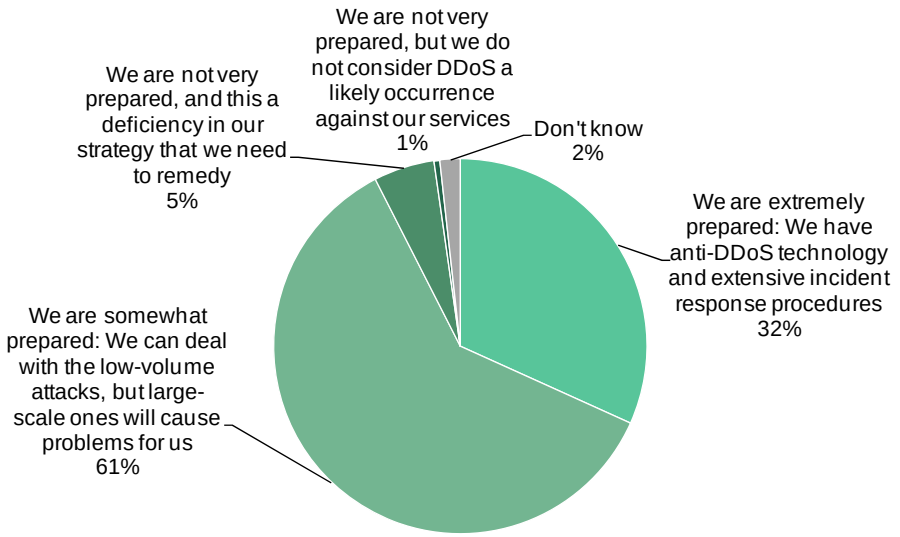
Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

Organizations Are Not Prepared for Large-Scale DDoS Attacks

When asked how prepared they think their organization is against DDoS threats, the majority of our respondents, 61 percent, indicated that they were prepared to deal with low-volume attacks but not large-scale ones. Another 6 percent said they were not very prepared (see Figure 17).

Figure 17: How Prepared Is Your Organization Against DDoS Threats?

"In your opinion, how prepared is your organization to deal with a large-scale DDoS attack?"



Base: 400 DDoS security professionals

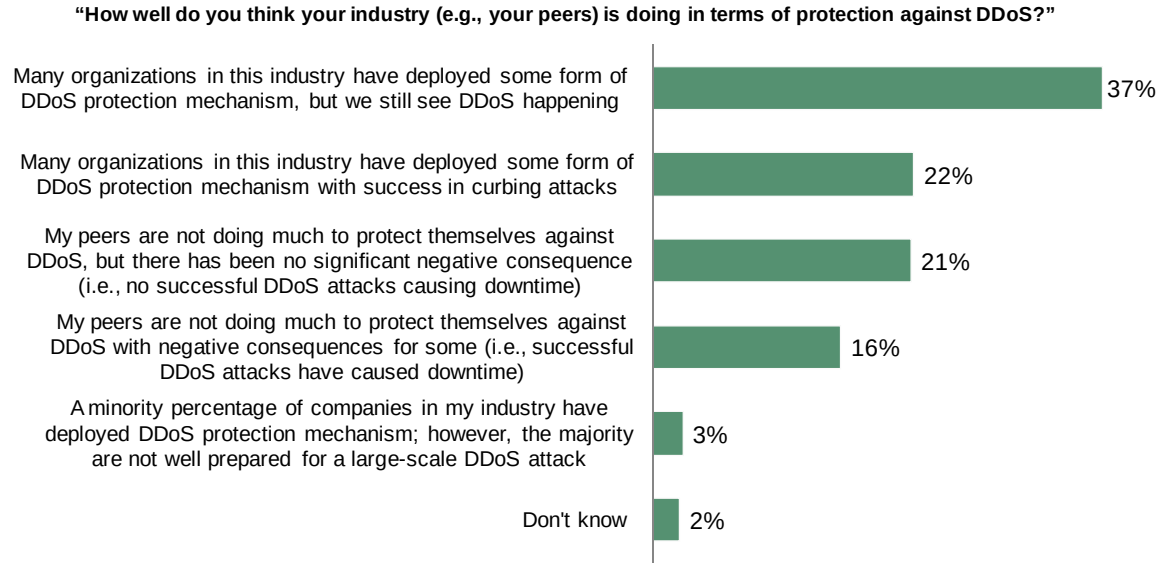
Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

Interestingly, 32 percent reported that they were extremely prepared for DDoS threats. However, a further inspection of the data revealed that 16.5 percent of those who responded with an "extremely prepared" answer had actually suffered from DDoS attacks that disrupted their services.

When we asked our respondents how satisfied they were with their current DDoS protection mechanism, 58 percent indicated they were "completely satisfied." This is somewhat surprising, considering none of the protection technologies proved to be infallible. It is even more surprising when compared to another survey question, "How well do you think your industry (your peers) is doing in terms of protection against DDoS?" Answers to the latter revealed that only 22 percent agreed that their peers were using DDoS protection with any form of success — a whopping 76 percent said either their peers are not doing much to prepare against DDoS attacks or not using DDoS protection with much success (see Figure 18).

Clearly, our respondents' self-assessment does not align with the opinions of their peers; 50 percent think they are doing a good job in their own organizations, while only 22 percent think their peers are doing a good job.

Figure 18: Peer Assessment Of Protection Against DDoS

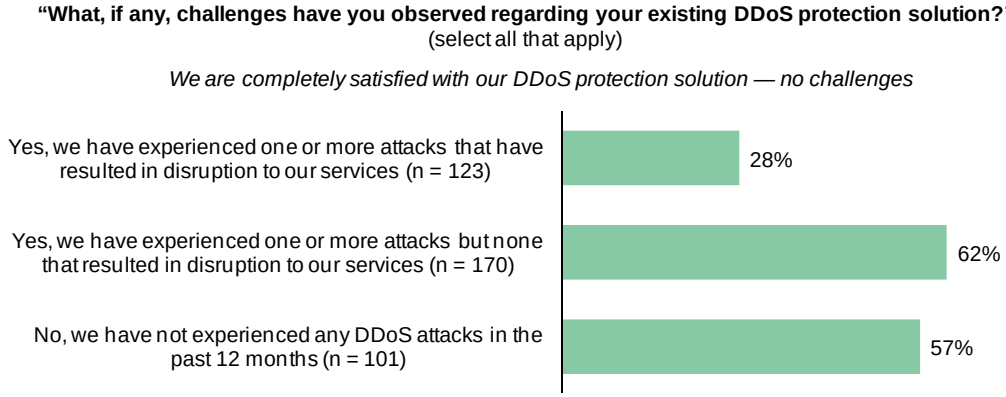


Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

This disparity can be further explained when we dig a little deeper in the self-assessment data. Twenty-eight percent of those who fell victim to a successful DDoS attack said they were "completely satisfied" with their DDoS protection mechanism (see Figure 19). These respondents seem to have an overblown sense of self-confidence in their DDoS protection mechanism, despite the evidence to the contrary. This overconfidence may have contributed to why most individuals think they are more prepared for DDoS than their peers assess their industry as a whole to be.

Figure 19: 28 Percent Of DDoS Victims Are Satisfied With Their Protection Method



Base: 400 DDoS security professionals

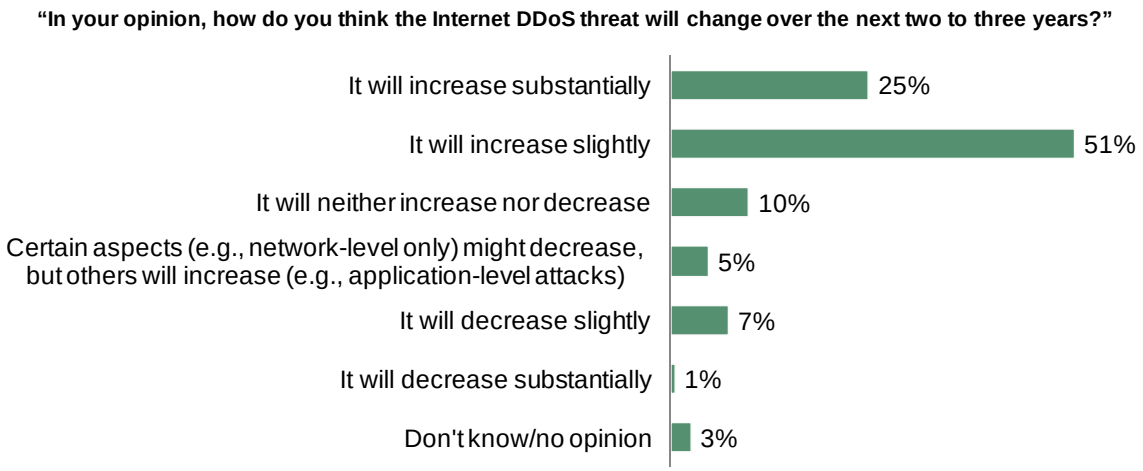
Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

Organizations Will Continue Investments In DDoS Protection Technologies

Many of our survey respondents believe that DDoS attacks will likely remain a credible threat for some time to come. When asked, "How do you think the Internet DDoS threat will change over the next two to three years?" 76 percent of respondents indicated that they believed the threat level would likely increase. Twenty-five percent believed the threat would increase significantly, while 51 percent predicted a slight increase in the threat level (see Figure 20).

Overall, our survey results showed a continued commitment toward DDoS protection. We asked our respondents whether their organizations' DDoS protection budget would increase or decrease for the next budget cycle. Nearly half, 49 percent to be exact, said their DDoS protection budget would increase, while 38 percent predicted it would remain the same (see Figure 21).

Figure 20: Future Threat Of DDoS Attacks

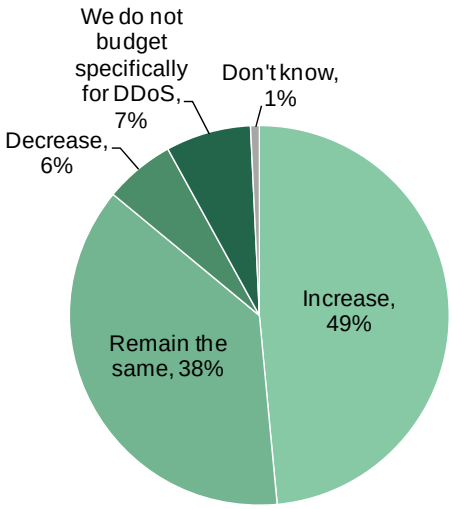


Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

Figure 21: Future Budget For DDoS Protection

"Do you predict that your organization's DDoS protection budget will increase or decrease in the next budget cycle?"



Base: 400 DDoS security professionals

Source: "Changing Landscape Of DDoS Threats And Protection," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 2009

Summary

As our study draws to a close, one thing is clear — organizations, big and small, are very much concerned about DDoS threats.

Though DDoS protection is widely practiced, few saw overwhelming success. Companies across the board revealed simultaneously high levels of confidence in their existing DDoS protection measures and the lack of concrete success evidence to back it up. Companies also expressed concerns over the viability of their ISPs in the face of large DDoS attacks — a valid worry considering that many companies saw their ISPs fall victim to DDoS attacks.

Overall, organizations agree that their peers and the industry as a whole are poorly prepared for large-scale attacks. Though evidence may suggest otherwise, most still prefer on-premise deployment as the main delivery method for anti-DDoS technologies. While most on-premise technology solutions today have the smarts to detect DDoS patterns, they lack the capacity and agility to rapidly mitigate attacks. As attacks seen in the wild continue to grow in size and sophistication, fewer and fewer organizations will have the ability to respond to DDoS in a successful manner. Forrester believes that companies that are seriously concerned about DDoS threats must investigate alternative means to protect their networks and online services.

Finally, many believe that DDoS attacks will remain a threat for the foreseeable future and that the industry will continue to invest in protection technologies. In contrast with the general economic downturn and the pressure for IT to do more with less resources, 87 percent of our respondents believe that their organizations will maintain or increase their current budget for DDoS protection in the foreseeable future.

Appendix A: Endnotes

[1] Source: “DDoS Protection,” a commissioned study conducted by Forrester Consulting on behalf of VeriSign, September 2008.

[2] Source: “DDoS Protection,” a commissioned study conducted by Forrester Consulting on behalf of VeriSign, September 2008.