IDG DDoS REPORT

EVOLVING STRATEGIES FOR HANDLING TODAY'S COMPLEX & COSTLY THREATS

CONTENTS

EXECUTIVE SUMMARY

This report summarizes research on distributed denial of service (DDoS) attacks focusing on trends and developments observed in 2018. Increasingly sophisticated DDoS attacks have become an inevitable part of the cybersecurity landscape threatening enterprise networks, Communication Service Providers (CSP), and their customers. As complex new challenges arise, more and more organizations are seeing the need to fortify their security posture.

2018 Survey Highlights >

2018 SURVEY HIGHLIGHTS:

86%

report experiencing **one or more** DDoS attack

Attack types are increasing in breadth and depth

DDoS attacks are distributed across multiple network layers and leverage multiple vectors — as before, **UDP Flood remains the most common and most frequently exploited** attack vector

Rapid detection and mitigation is the main consideration for selecting a DDoS solution

Technical complexity is reportedly the number one barrier to bolstering DDoS protection

83%

consider their current solutions highly effective in managing large-scale attacks

Respondents report a preference for on-premises appliances to address multi-vector threats

70%

are highly likely to consider changing their current solution, in contrast to high effectiveness ratings

49%

respondents anticipate increasing their budgets to address DDoS threats

More than half of respondents offer hosted services to third parties, and 2/3 of those offer DDoS prevention services

The majority holds CSPs equally or more responsible for DDoS prevention when applications are deployed via a cloud service provider

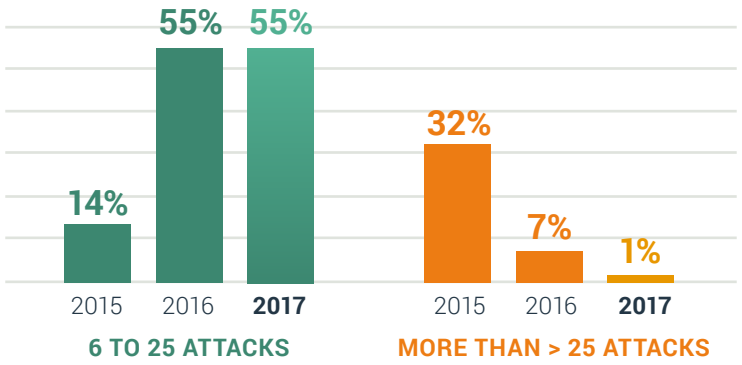
The emergence of 5G poses serious new security challenges for mobile service providers

ONE OR MORE SERIOUS ATTACK PER RESPONDENT

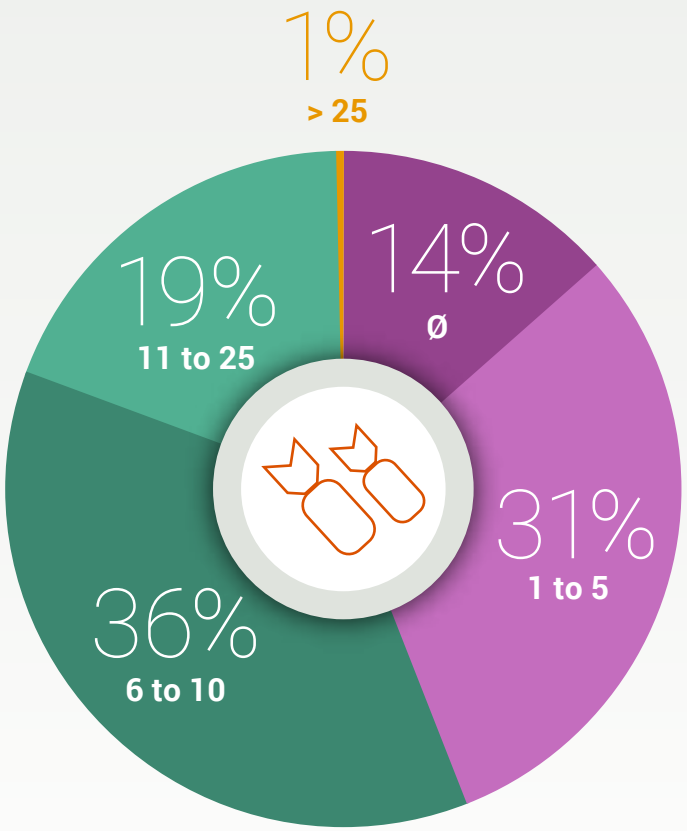
DDoS attacks have increased in sophistication and intensity, threatening the availability of enterprise services, applications, websites, and networks.

Most survey respondents (86%) report experiencing at least one DDoS attack in the past 12 months.

*NUMBER OF DDoS ATTACKS – **OVER TIME***



*NUMBER OF DDoS ATTACKS – **PAST 12 MONTHS***

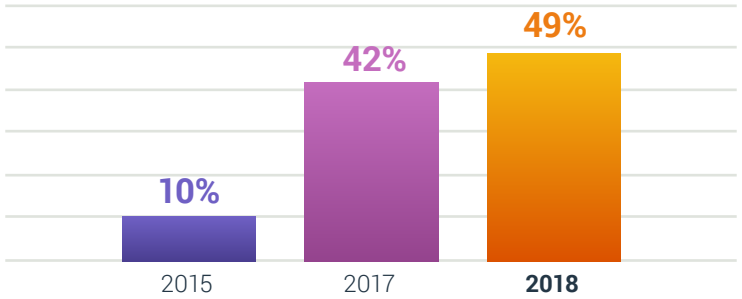


SIZE AND MAGNITUDE HAVE GROWN SIGNIFICANTLY

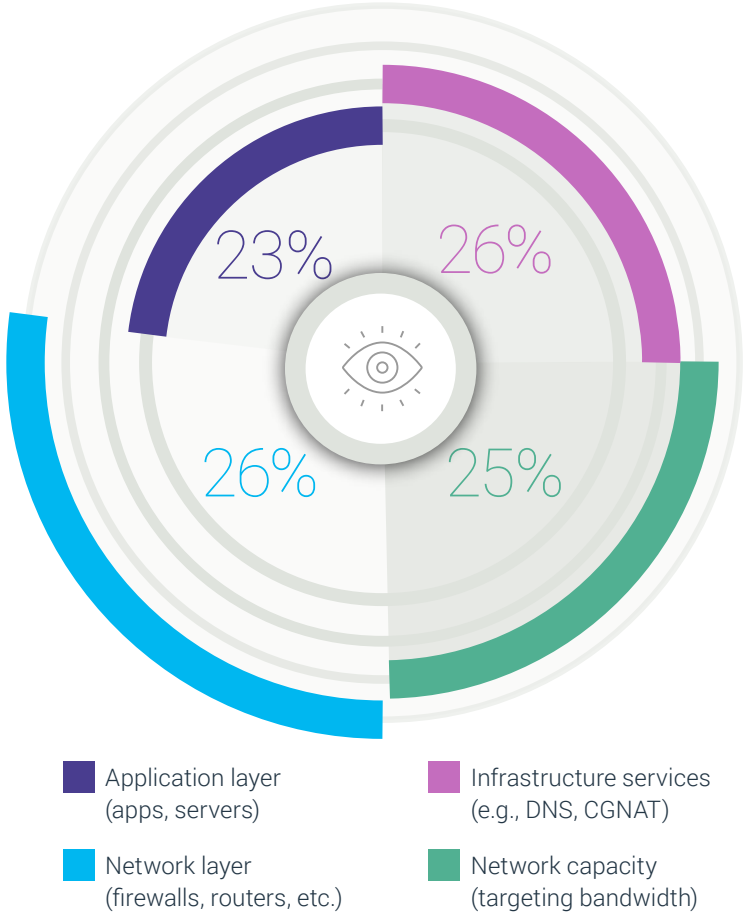
Attack types are increasing in breadth and depth.

In 2018, 49% of survey respondents reported an average DDoS attack size of greater than 50 Gbps, while only 10% reported the same in 2015. The research shows that attack types are increasing in breadth and depth, distributed across multiple areas of IT infrastructure in nearly equal proportions.

***AVERAGE** DDoS ATTACKS >50 GBPS*



PERCENT OF DDoS ATTACKS
TARGETING EACH AREA

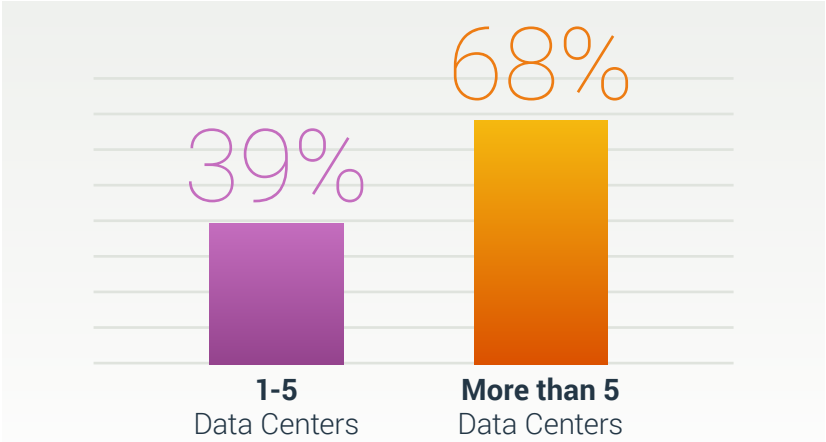


MULTIPLE DATA CENTERS: A TARGET-RICH ENVIRONMENT

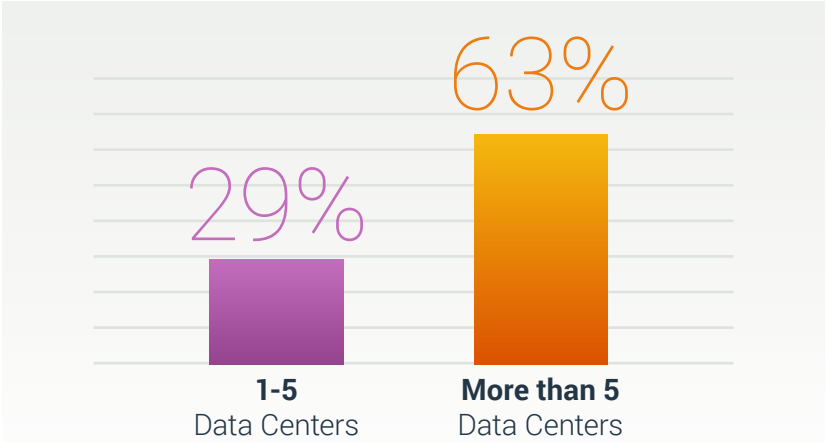
Once attackers have identified a good target, they are apt to continue probing other data centers in the same "family." Consequently, the more data centers an organization operates, the greater its likelihood of being attacked.

Attacks are launched for a variety of reasons. Some are just the result of random opportunism — thrill-seeking attackers. In some cases, state-sponsored actors seek to disrupt operations of foreign adversaries or business competitors. Others are driven by activists looking to raise awareness for a "pet" cause, be it social or political. And some attacks are used as a cover for more malicious, intrusive hacks. Whatever the reason, organizations with more than five data centers are more frequently targeted, and the average attack size is considerably larger.

*EXPERIENCED **5 OR MORE** DDoS ATTACKS*



*AVERAGE DDoS ATTACK **>50 GBPS***

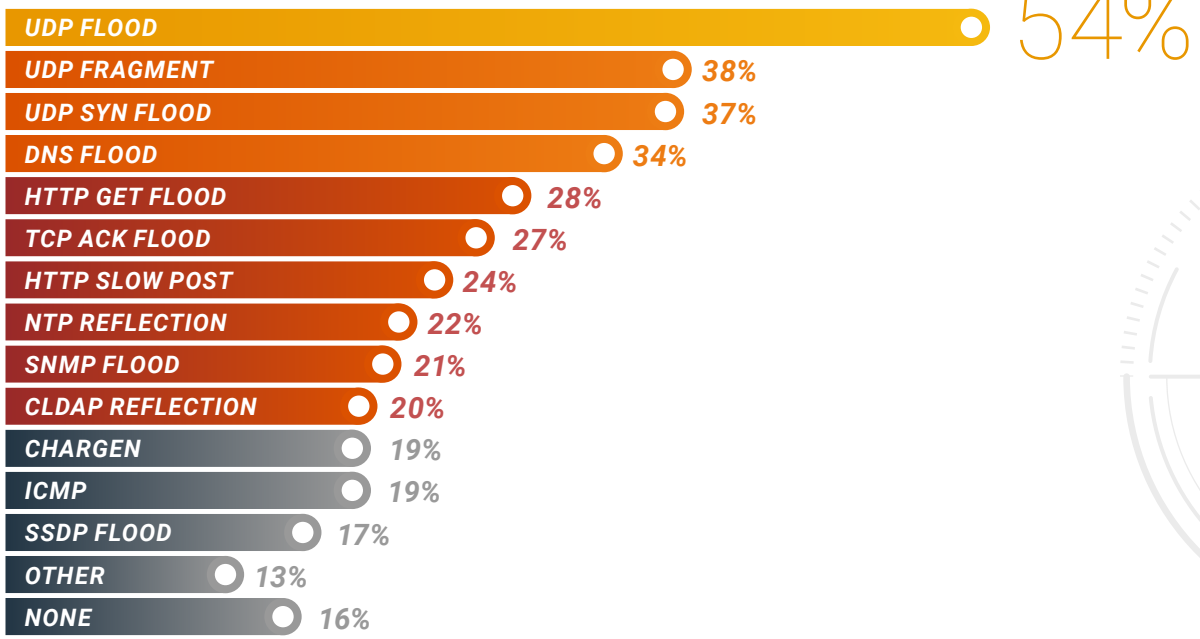


UDP FLOOD CONTINUES TO LEAD THE PACK

Attackers exploit multiple vectors to launch their DDoS attacks.

As in our previous survey, UDP Flood (including DNS Amplification) was the attack vector most frequently leveraged against respondents' organizations in the past 12 months. While the overall mix of vectors remains relatively stable, the scale increased dramatically with all categories up significantly from the last survey.

PERCENT REPORTING ***ATTACK VECTOR WAS LEVERAGED***



MEASURING THE IMPACT OF DOWNTIME

The average downtime per attack grows as the number of DDoS attacks increases, indicating inefficient mitigation processes. While respondents cite a number of factors by which they gauge the impact, the top response is Time to Service Restoration.

What accounts for the difference? It depends on who's responding. Whereas CSOs may see service restoration time as the most important metric, CIOs will see order-processing uptime as critical. CEOs are apt to be more concerned about hits to a company's reputation seen in the press. Business priorities vary by organization, and by the teams within them. One may see customer satisfaction as the primary goal, while keeping the back office up and running as secondary. DDoS mitigation strategies should be subjected to rigorous reviews against changing business priorities and the evolving nature of threats to ensure they continue to meet business objectives.

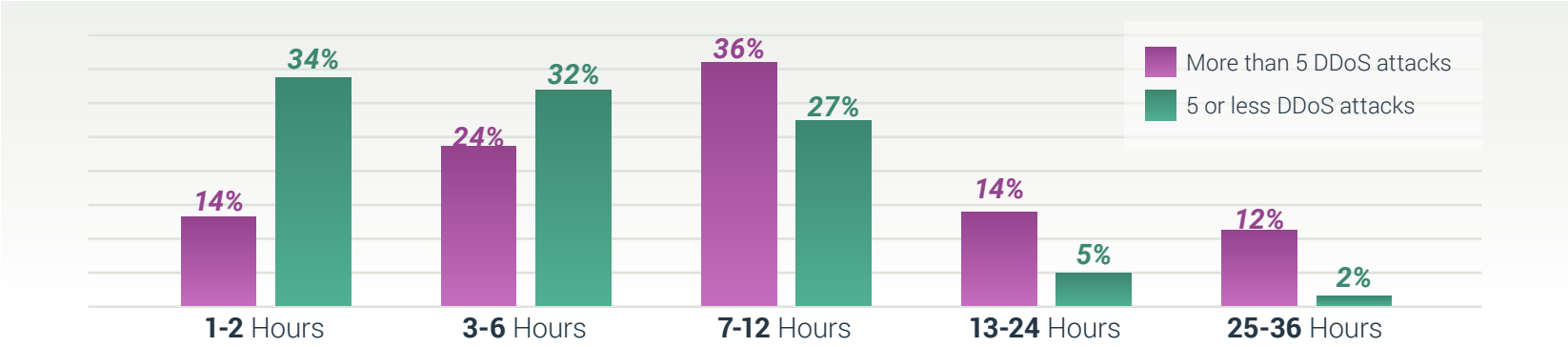
71% *Time to Service Restoration*

52% *Customer Satisfaction*

47% *Order Processing*

36% *Press Coverage/ Company Reputation*

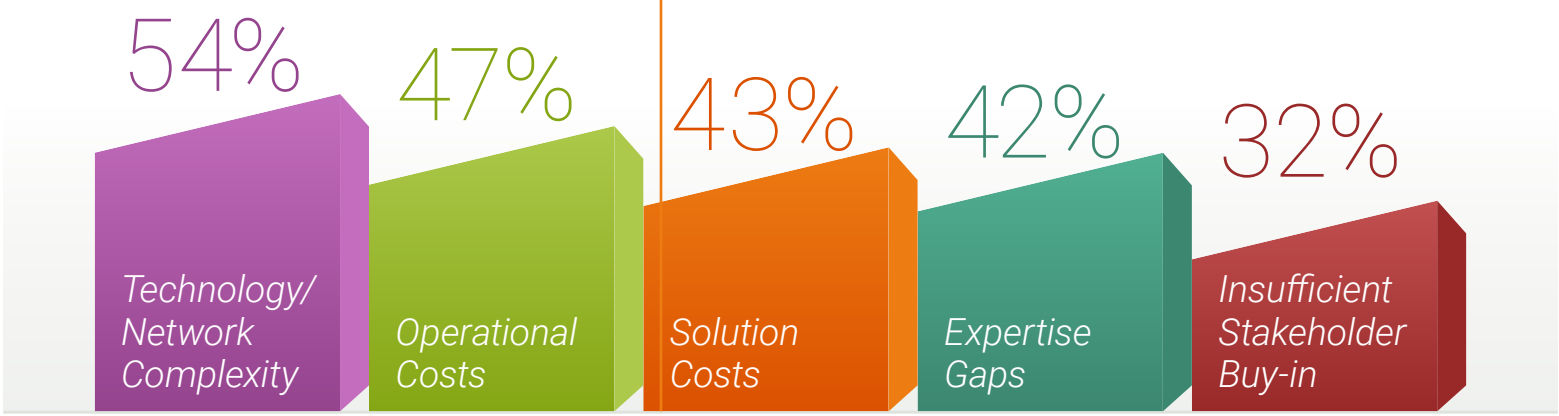
AVERAGE DOWNTIME



OBSTACLES TO ACHIEVING BETTER PROTECTION

Despite the positive reviews for current DDoS solutions, respondents do report limitations. In the current survey, keeping up with the complex array of attack types is identified as the number one barrier to greater DDoS protection:

Respondents at organizations with a **planned budget increase** to address multi-vector DDoS threats are more likely to cite the *cost of detect and mitigation solutions* as a barrier (52% vs. 33% among all others).



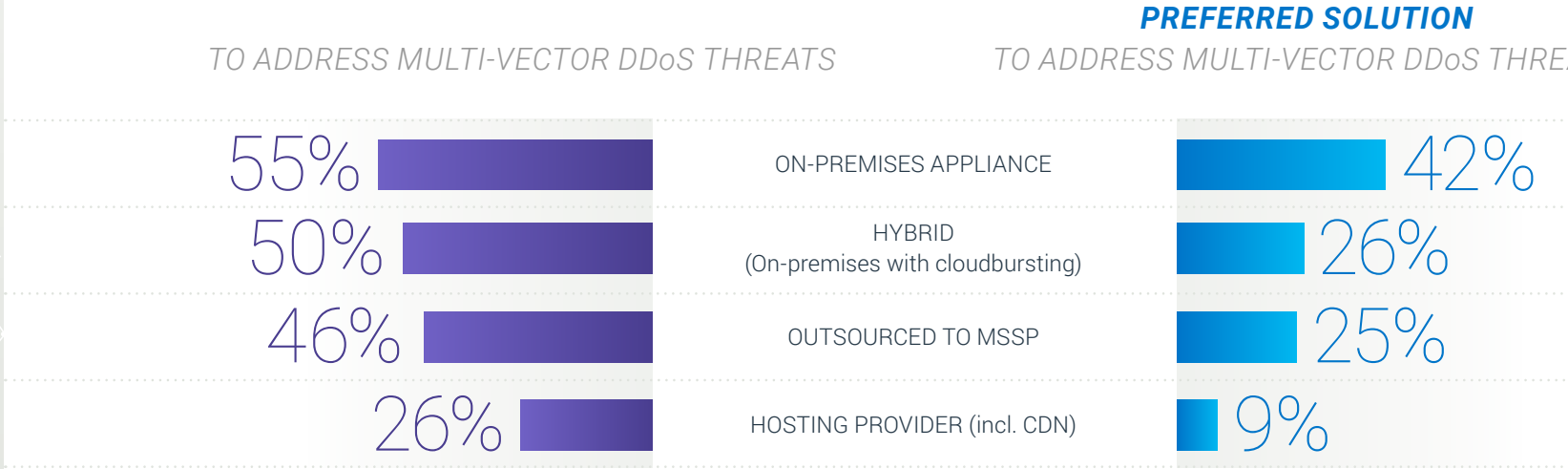
INTERNAL BARRIERS TO GREATER DDoS PROTECTION

ON-PREMISES APPLIANCES: THE PREFERRED SOLUTION

While more than half (53%) of respondents have two or more solutions in place, their preference is clearly for on-premises appliances over other solution types.

Appliances are increasingly seen as the most effective way to address multi-vector DDoS threats and are more likely to be rated "extremely effective." However, as appliance use has increased, it appears that the proportion of other solutions in place remains largely unchanged, suggesting that appliances are being brought in to reinforce existing protection, rather than to replace it.

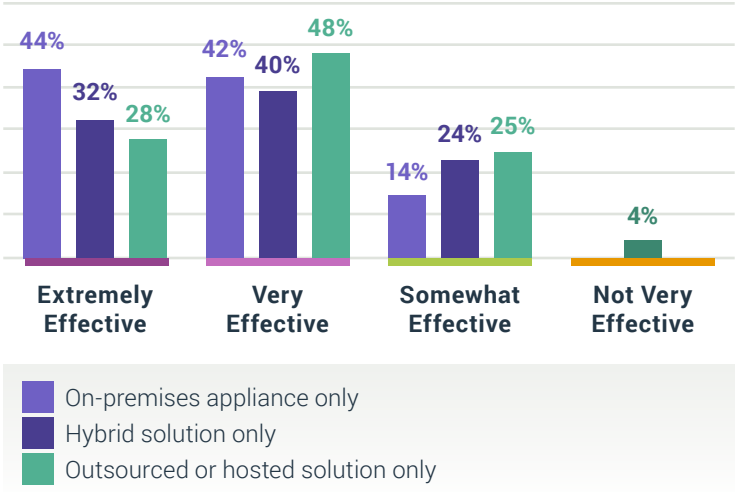
53%
HAVE 2 OR MORE SOLUTIONS IN PLACE



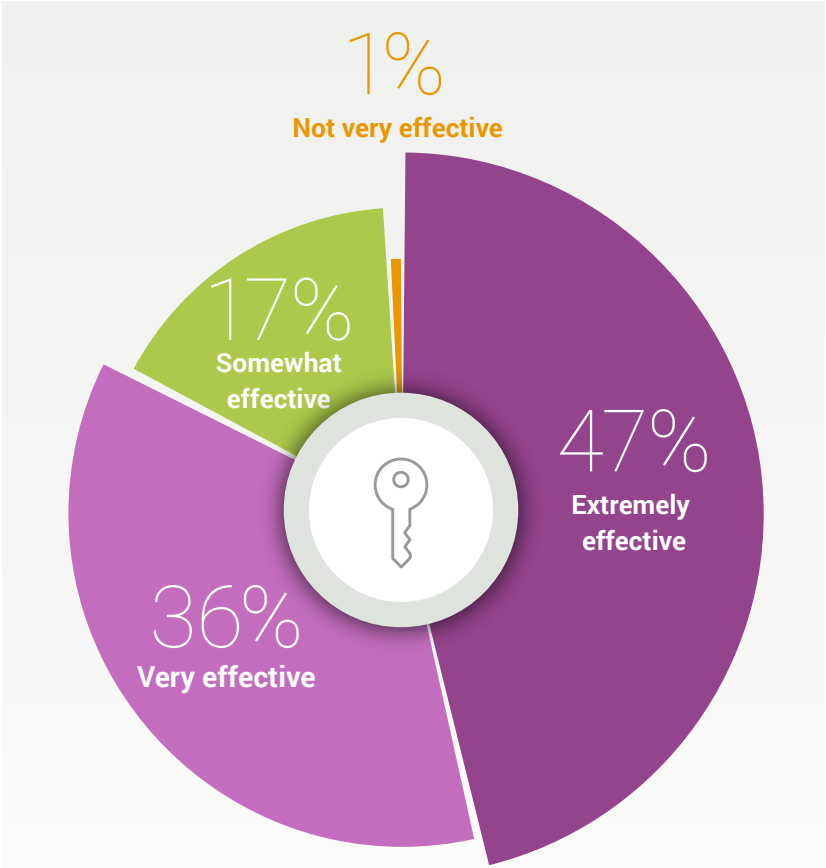
MOST SEE THEIR CURRENT SOLUTIONS AS HIGHLY EFFECTIVE

When it comes to managing large-scale, multi-vector attacks, **83% of respondents consider their current DDoS protection solutions to be highly effective.** As noted previously, on-premises appliances are more likely to be rated "extremely effective." The confidence expressed in current solutions is likely due to the fact that organizations are, on average, experiencing less downtime from DDoS attacks. In 2015, 29% of respondents reported average downtime of 25 hours or more, compared to only 8% in 2018. Over the past few years, downtime has shifted from being measured in days to hours and minutes.

*EFFECTIVENESS BY **TYPE OF SOLUTION** IN PLACE*

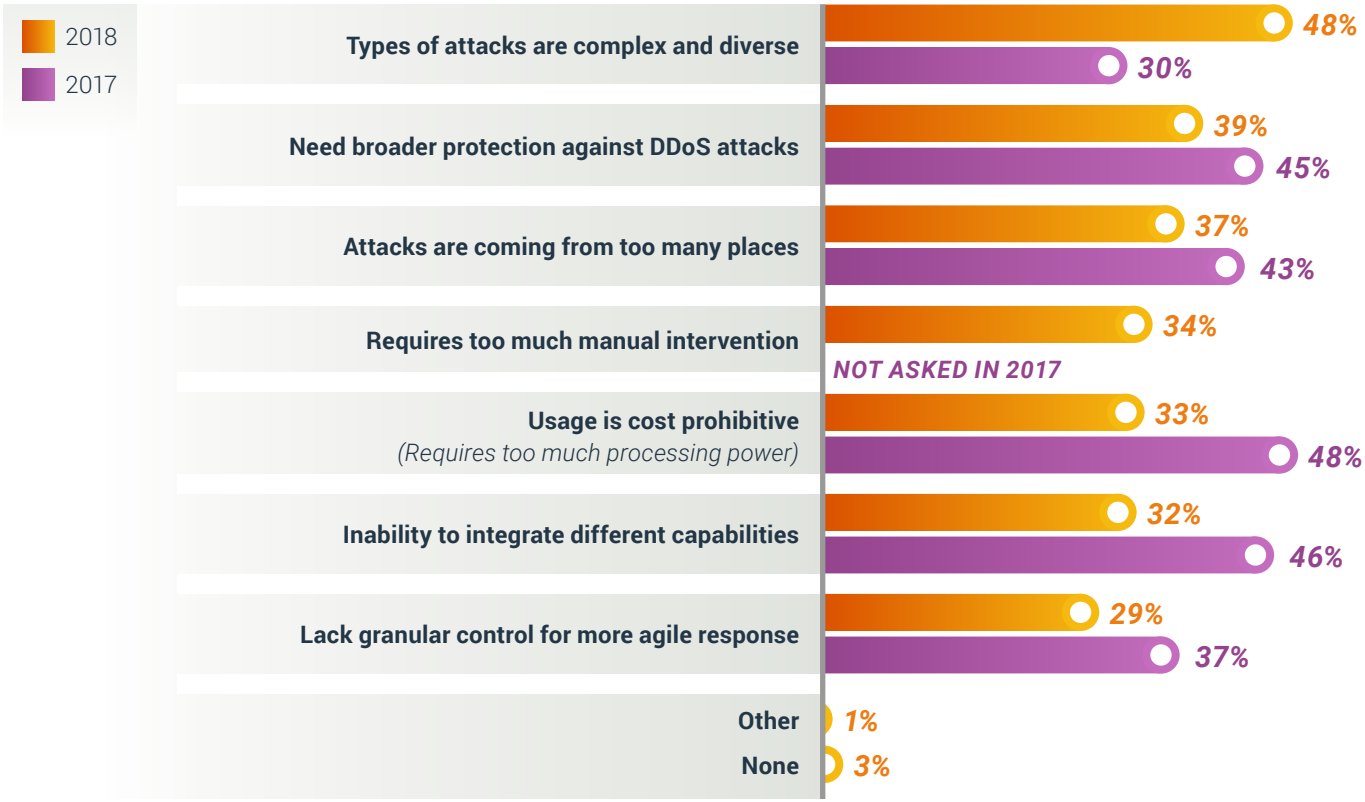


EFFECTIVENESS OF CURRENT DDoS PROTECTION



PROVIDING EFFECTIVE PROTECTION IS AN ONGOING CHALLENGE

In the current survey, keeping up with evolving and ever-proliferating attack types and methods is identified as the key challenge to implementing more effective DDoS protection. The increasing complexity of attacks coupled with increasingly complex, hybrid infrastructures make the cyber-threat landscape more opaque than ever before. As in 2017, usage cost continues to be an important consideration. All in all, the challenges have become less daunting on a year-over-year basis, pointing to the increased efficacy and ease-of-use of DDoS solutions.

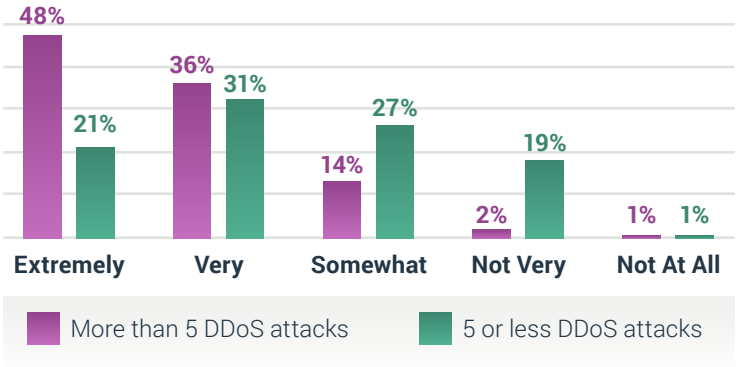


SATISFIED, YES!
BUT ALSO OPEN TO CHANGE

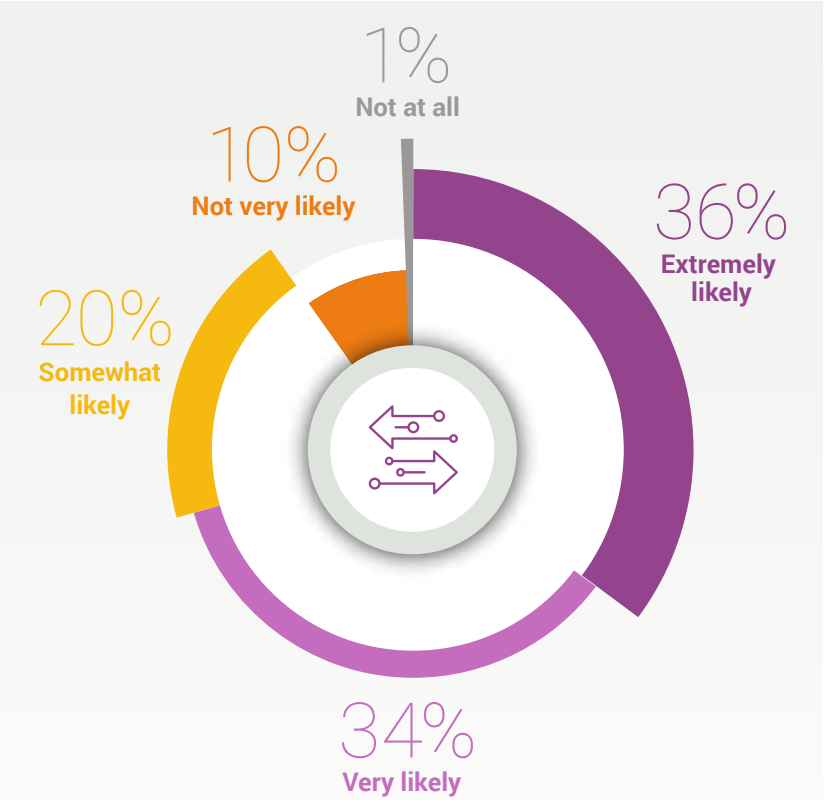
Despite rating their existing solutions highly effective, seven in ten respondents (70%) report a high likelihood to consider a change to their DDoS solution currently in place.

The likelihood to switch correlates positively to the number of attacks experienced. More attacks equal a greater propensity to try something different. 48% that experienced five or more attacks said they're extremely likely to consider a switch.

*LIKELIHOOD TO CONSIDER A CHANGE – **BY THE NUMBER OF DDoS ATTACKS EXPERIENCED***



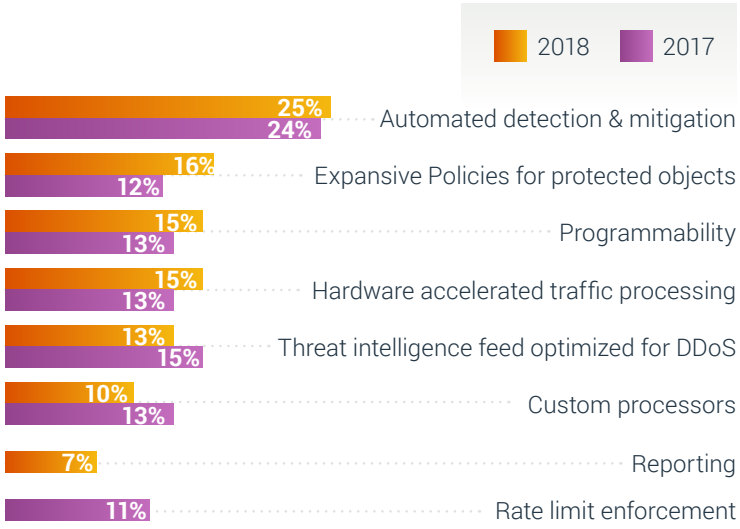
*LIKELIHOOD TO CONSIDER A CHANGE TO DDoS SOLUTION – **NEXT 12 MONTHS***



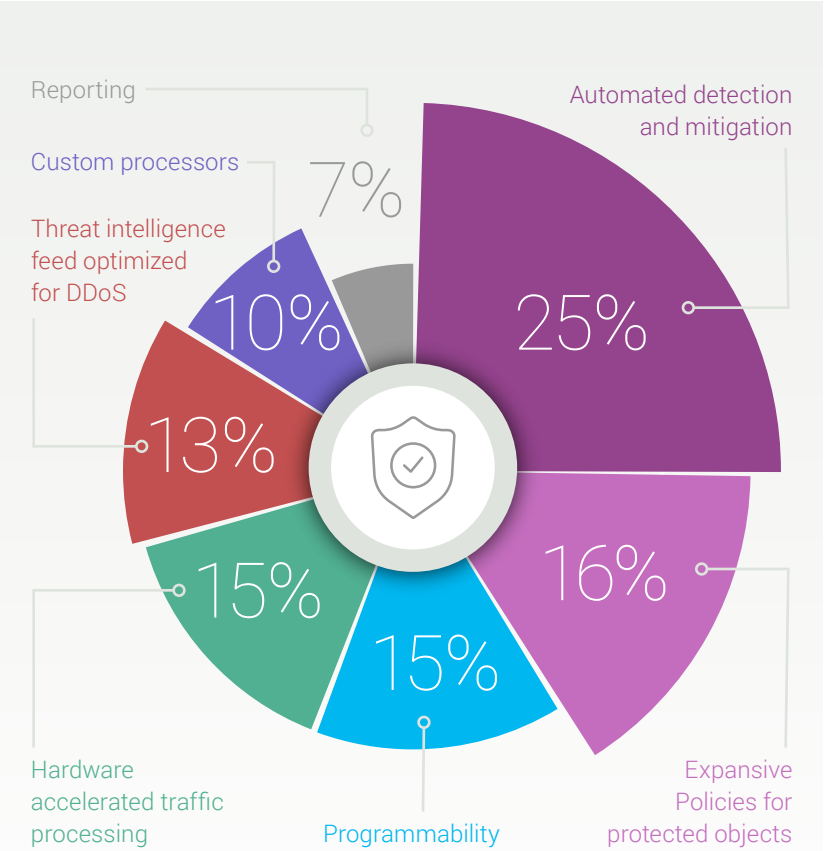
AUTOMATION TOPS THE LIST

The DDoS market is maturing, with more advanced capabilities frequently coming online.

Automated detection and mitigation is still the number one feature considered when selecting a DDoS solution, up just a touch over 2017. In general, there have been no major shifts in opinion over the past year regarding the top desired anti-DDoS features and capabilities.



2018 FEATURE OR CAPABILITY MOST IMPORTANT *IN A DDoS SOLUTION*

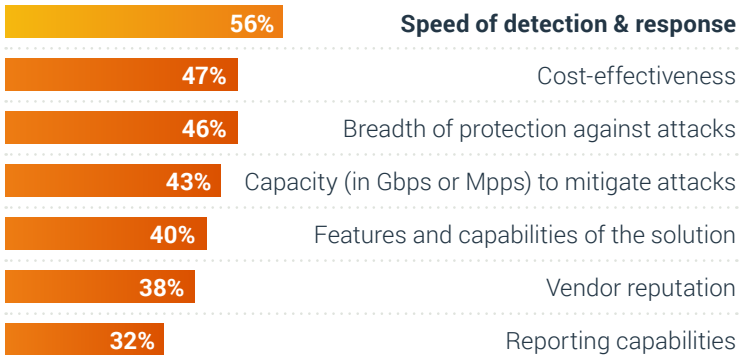


THE NEED FOR SPEED

Speedy response is what respondents want most in a DDoS solution.

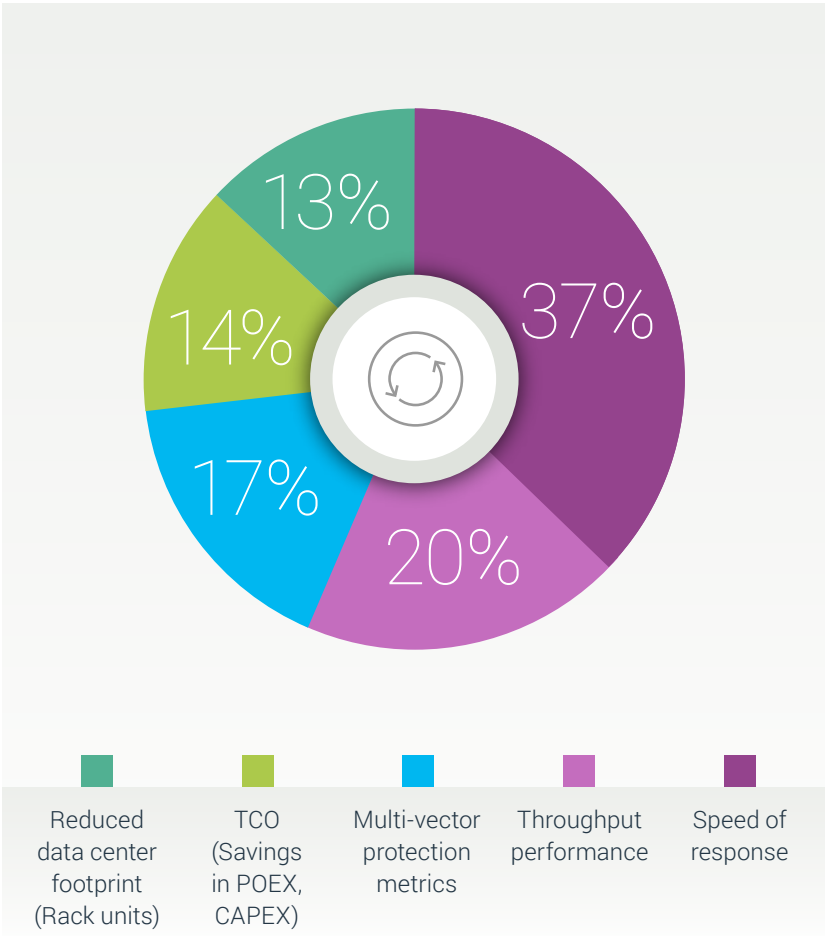
Speed of detection and remediation also rises to the top of the list when they are asked to rank solution selection criteria. Executives with the title of CEO, President, or Owner are more likely to rank "cost-effectiveness" among their top three criteria (55% versus 34% for respondents with other titles). While cost appears to be a top-of-mind concern, it's interesting to note that, nevertheless, nearly one-half of respondents plan to increase their DDoS budget in the coming year. Clearly, they see the need to keep their level of protection effective and up to date.

IMPORTANCE OF CRITERIA
*WHEN SELECTING A DDoS SOLUTION**



*% Ranking Criteria in the Top 3

MOST IMPORTANT POTENTIAL BENEFIT
OF A DDoS SOLUTION

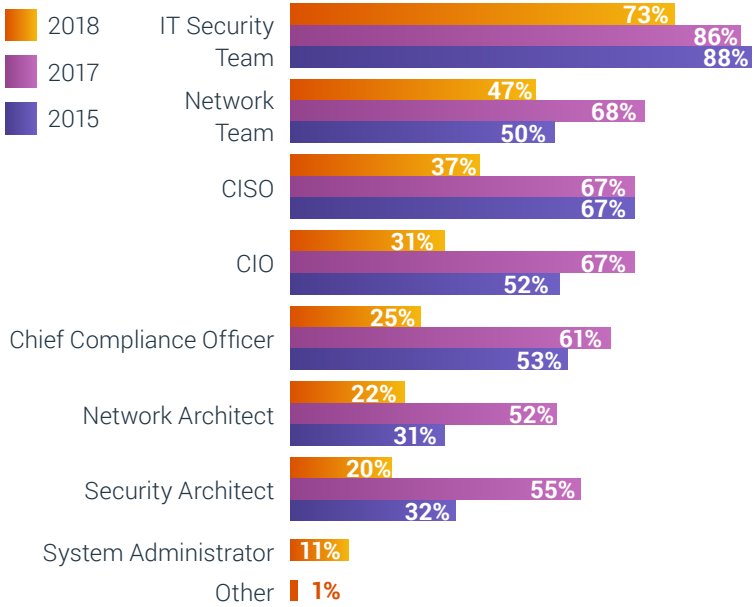


DEFENSE BUDGETS UP 24%

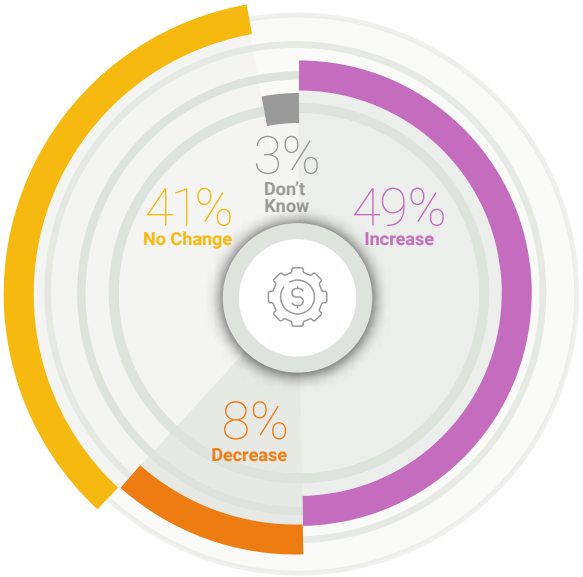
Nearly one-half of respondents (49%) anticipate increases in their organizations' budgets to address DDoS threats. Budgets are expected to increase by 24% on average. While IT security teams still top the list in terms of responsibility for DDoS prevention, many other roles including network administrator, security architect, and network architect have increased in importance since 2015.

Skills and experience across the workforce are increasing, calling for expanded security budgets. Provisioning protection that is in synch with evolving business objectives and capable of taking on new and emerging DDoS threats is clearly a top priority. The fact that cost is seen as a barrier, yet budgets are increasing, suggests that decision makers are working harder to secure funding.

INDIVIDUALS RESPONSIBLE
FOR DDoS PREVENTION EFFORTS



EXPECTED CHANGE IN BUDGET
TO ADDRESS MULTI-VECTOR DDoS THREATS

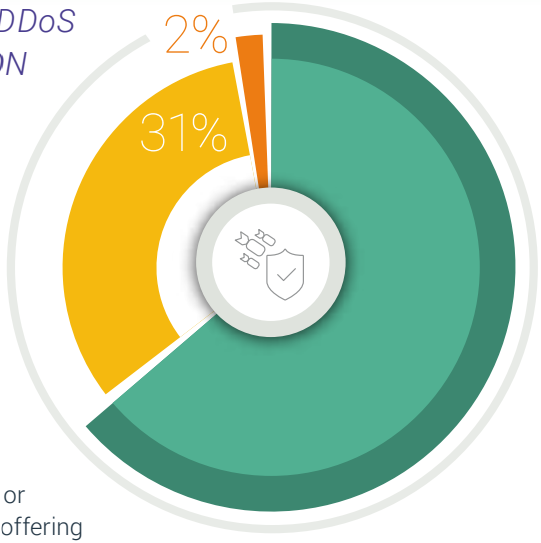


WHO'S RESPONSIBLE FOR DDoS PREVENTION?

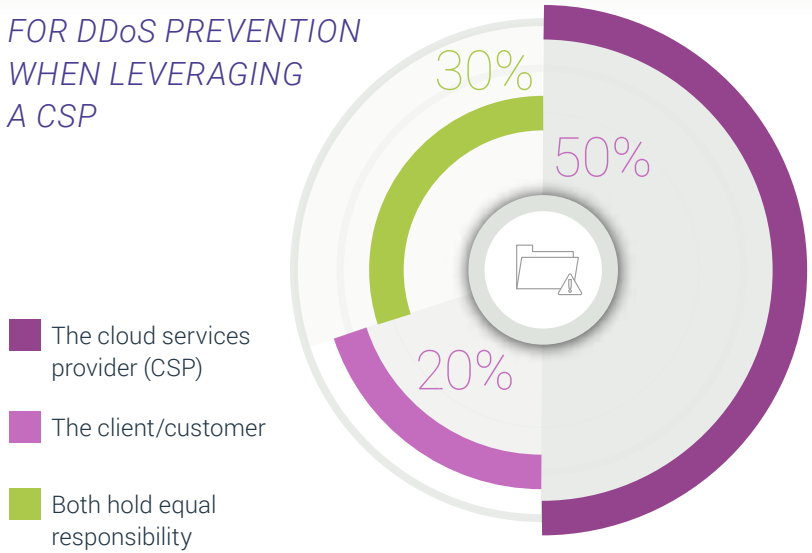
More than half (55%) of survey respondents offer hosted services to third parties, and two-thirds of those offer DDoS prevention services. Most respondents believe that service providers hold at least equal responsibility for DDoS prevention when applications are deployed via cloud service providers, while one-half (50%) believe service providers bear the main responsibility.

The evolution of DDoS methods suggests that CSPs need to enhance their security posture and find better ways to protect critical infrastructure and their tenants. The continued discovery of new attack patterns should also prompt enterprises to seek DDoS-proof service providers. The advent of 5G is forecast to drive exponential growth in connected IoT devices, dramatically expanding attacks via DDoS botnets. Analysts predict that DDoS will go hyper-scale with 5G. To protect their networks and customers from these rapidly growing threats, mobile service providers will need to leverage sophisticated DDoS threat intelligence and advanced, automated detection and mitigation solutions.

***OFFERING OR CONSIDERING OFFERING** DDoS PREVENTION SERVICES*



***PRIMARY RESPONSIBILITY** FOR DDoS PREVENTION WHEN LEVERAGING A CSP*



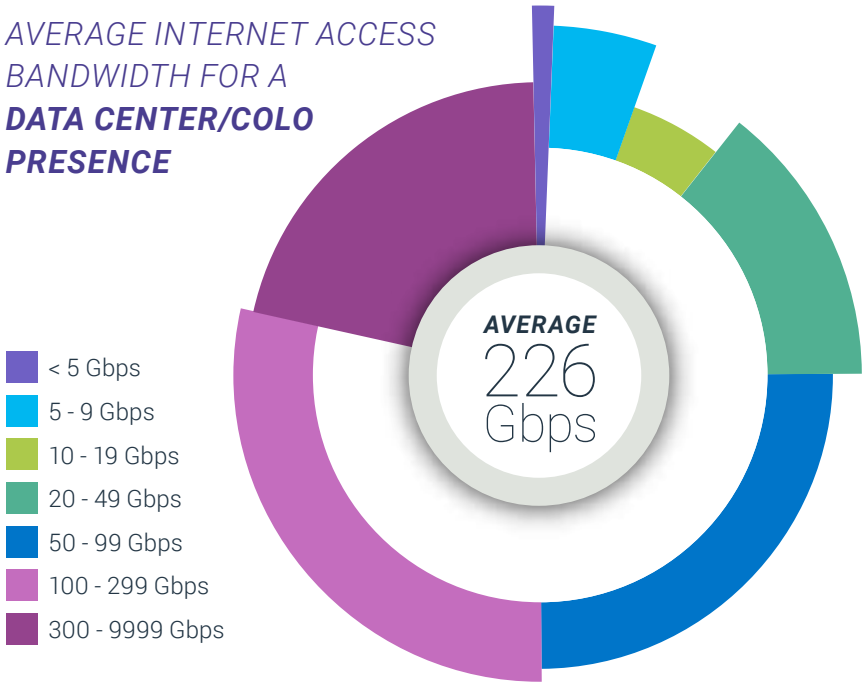
ABOUT THE SURVEY

The IDG Connect research survey was conducted on behalf of A10 Networks in order to analyze the cybersecurity landscape, especially as it pertains to DDoS threats across select industries. Via an online questionnaire, 200+ respondents from the US and UK were queried at organizations averaging 6,316 employees. 35% were software, computer services, telecommunications, and engineering organizations.

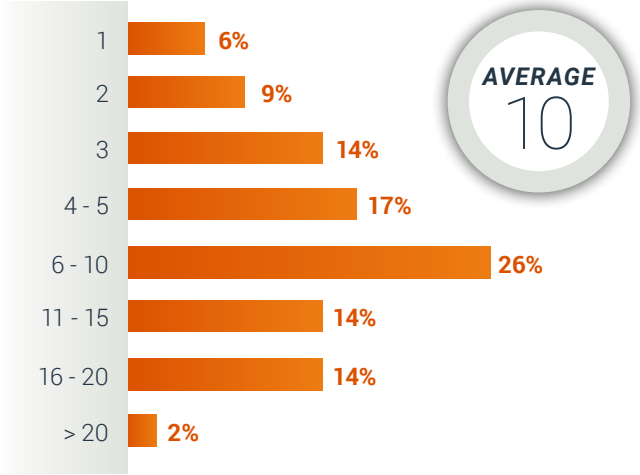
Respondent profiles:

- Responsibility or oversight for application service delivery, IT networking or IT security
- CEOs (27%), CIOs (18%), and IT security executives and staff (35%)
- Knowledgeable of:
  - Average Internet access bandwidth
  - Number of data centers in operation
  - Number of DDoS attacks experienced over the past 18 months

AVERAGE INTERNET ACCESS BANDWIDTH FOR A ***DATA CENTER/COLO PRESENCE***



NUMBER OF ***DATA CENTERS IN OPERATION***



DOWNLOAD
eBOOK

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information visit:

a10networks.com

or tweet
@A10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-EB-14116-EN-01 FEB 2019