# DDoS: STRATEGIES FOR DEALING WITH A GROWING THREAT

IDG CONNECT

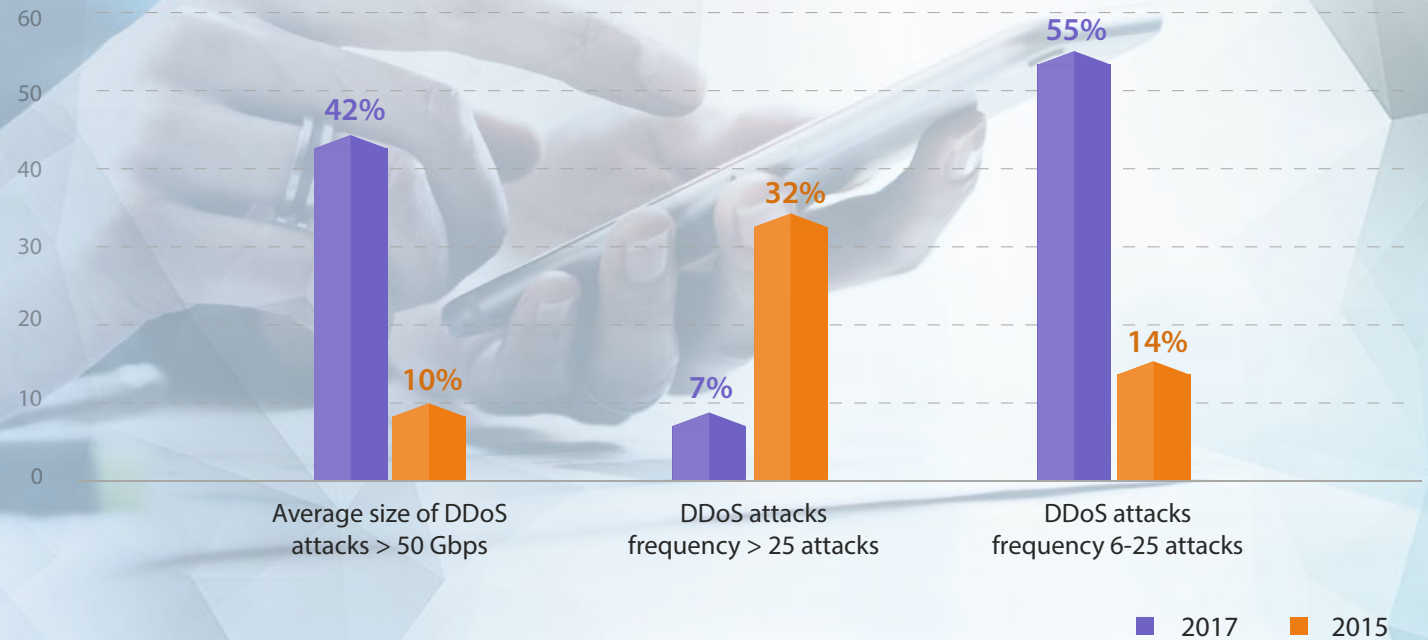
# 01. EXECUTIVE SUMMARY

This report summarizes recent research on distributed denial of service (DDoS) attacks, which looks at data collated recently and compares some of this data to a similar study conducted in 2015. Overall, DDoS attacks have done the cyberthreat equivalent of "going mainstream". Increasingly sophisticated DDoS attacks have become an inevitable part of the cybersecurity landscape, threatening the availability of enterprise websites. While the challenge from such attacks remains greater than ever, the market is maturing and organizations recognize that they need to deliver an appropriate response.

**Key findings from the research are as follows:**

- The scale of DDoS attacks has increased by an order of magnitude, reaching over 1 Tbps in some cases. In 2015, only 10% of average attacks were above 50 Gbps, in 2017 the average size of attacks greater than 50 Gbps quadrupled to 42%.
- Attacks are more widely distributed. Whereas 32% of organizations experienced more than 25 attacks in 2015, this figure has dropped to 7% for 2017. The number of organizations experiencing between 6 and 25 attacks has increased to 55%, from 14% in 2015.
- While network layer attacks are more prevalent, DDoS attacks remain varied and multi-targeted, Network layer DDoS attacks are the most common, with 29% of respondents encountering attacks at the network level.
- Organizations are moving away from hybrid solutions and toward on-premise appliances to counter multi-vector attacks. Focus is increasingly on vendor performance and solution effectiveness rather than any particular feature set.
- DDoS protection is perceived as effective across the organizations surveyed. Downtime is moving away from being measured in days to being measured in hours.
- Alongside performance guarantees, technology decision makers are seeing cost effectiveness as a key criterion for DDoS solutions. In parallel with budgets increasing, solution and operational costs are seen as the number one internal barrier to increasing the level of DDoS protection.
- An increasingly cross-functional, experienced pool of stakeholders are involved in DDoS prevention efforts. This is impacting the criteria used to define downtime and resolution.
- The DDoS threat landscape continues to evolve, leaving no room for complacency. Above all, organizations need to decide what criteria are most appropriate to their business needs and set their DDoS strategy and solutions accordingly.

# 02. DDoS THREATS HAVE GROWN RAPIDLY AND CAN NO LONGER BE IGNORED




Increasingly sophisticated DDoS attacks have become an inevitable part of the cybersecurity landscape, threatening the availability of enterprise services, applications and websites. Since we ran this research two years ago, attacks have grown by an order of magnitude, with the scale of such attacks increasing to beyond 1 Tbps in certain cases.

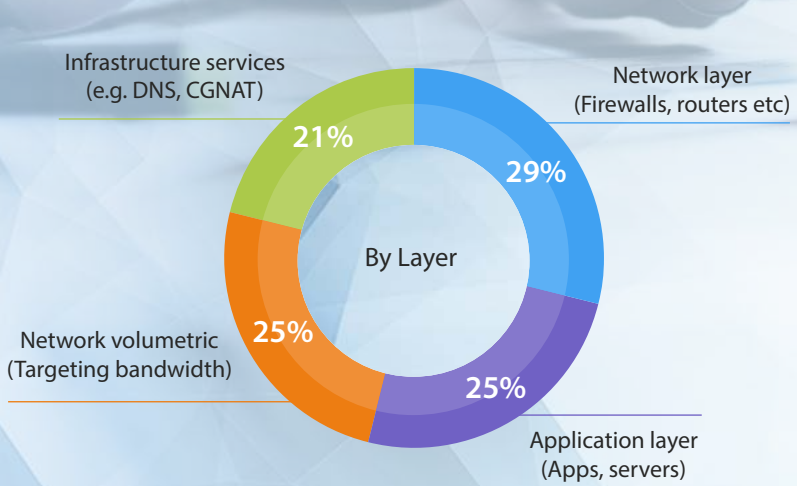
As the figure shows, in 2015 only 10% of attacks were above 50 Gbps, whereas this figure has now increased to 42%. Interestingly, attacks are more widely distributed: where 32% of organizations experienced more than 25 attacks in 2015, this figure has dropped to 7%, while the number of organizations experiencing 6 to 25 attacks has increased to 55% from 14% in 2015.

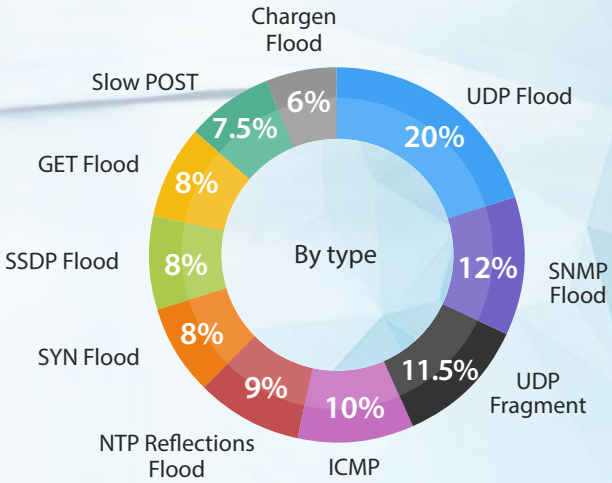
# 02. DDoS THREATS HAVE GROWN RAPIDLY AND CAN NO LONGER BE IGNORED

At the same time, the research shows how attack types are increasing in breadth and depth. Businesses experienced a significant percentage of all listed multi-vector DDoS attacks. Network layer DDoS attacks, which target network components such as firewalls and routers, are most prevalent, with 29% of respondents encountering attacks at the network level.

This picture is relatively unchanged from 2015, as is the variance on the types of attacks experienced. The highest relative percentage of organizations faced UDP flood attacks (including DNS amplification). Overall, the vectors may be evolving gradually over time, but the scale is increasing dramatically.

**Multi-Vector DDoS Attack Breakdown**



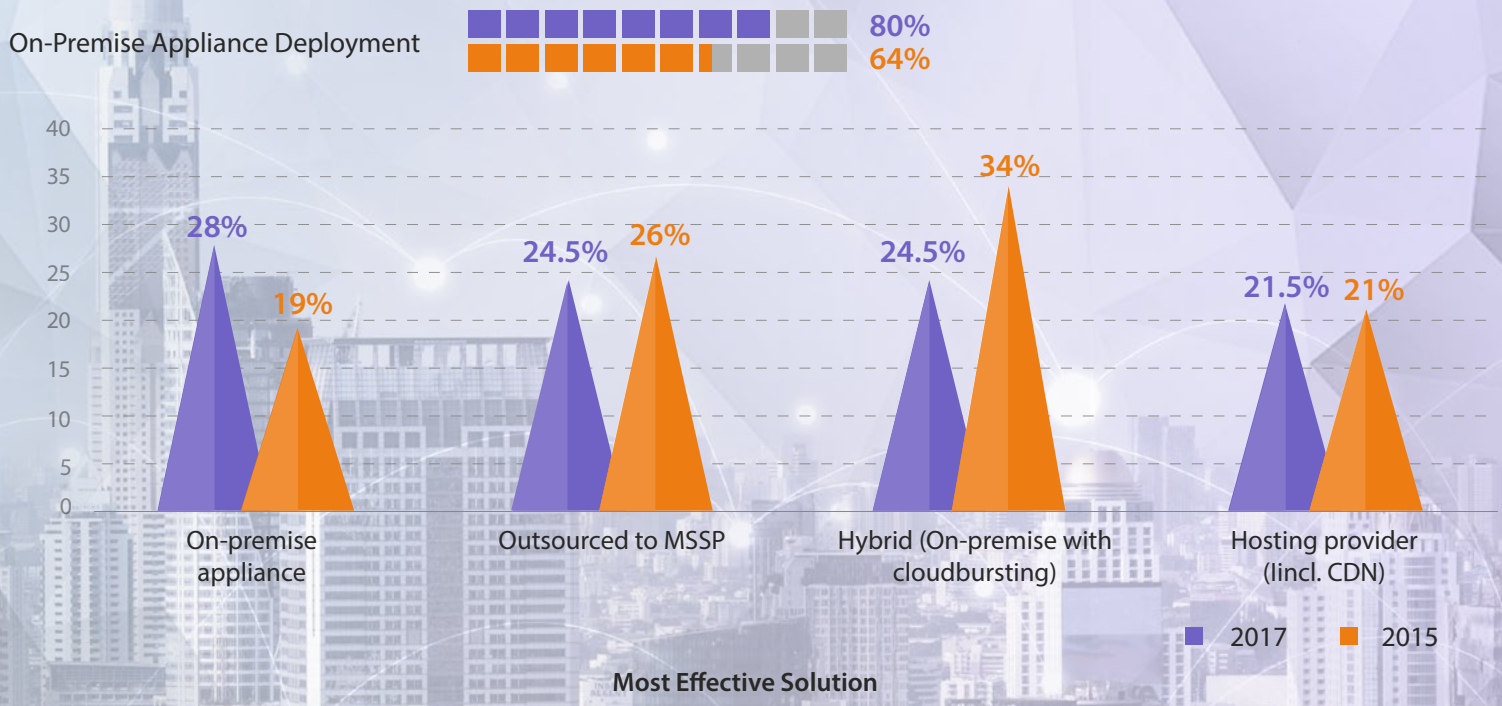

Percentage of respondents

IDG CONNECT

# 03. THE DDoS MARKET IS MATURING, WITH MORE ORGANIZATIONS WITH SOLUTIONS IN PLACE

Organizations are aware of the DDoS threat, and are prepared to deploy solutions in response. We gain an insight into this maturing market by looking at the kinds of solutions being deployed: on-premise appliances are now installed at 80% of respondent organizations, compared to 64% two years ago. Appliances are increasingly seen as the most effective way to address multi-vector DDoS threats, increasing from 19% to 28% over two years, whereas hybrid solutions have decreased by a similar proportion.

While appliance use has increased, it appears as though other solutions in place remain largely unchanged. This suggests that appliances have been brought in to reinforce existing protection, rather than to replace it.

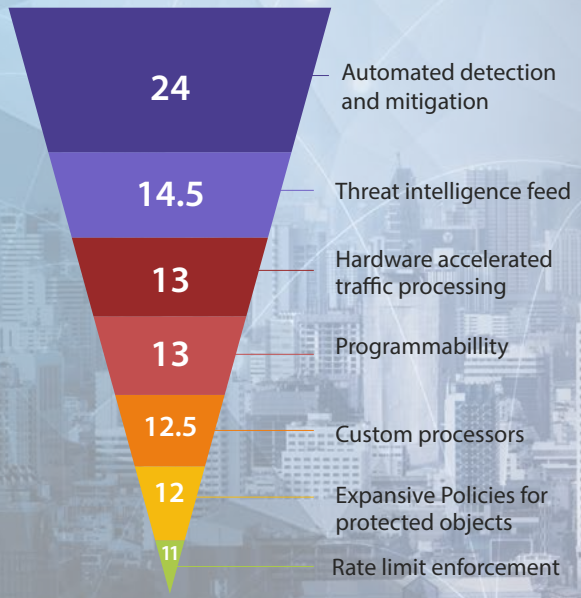


# 03. THE DDoS MARKET IS MATURING, WITH MORE ORGANIZATIONS WITH SOLUTIONS IN PLACE

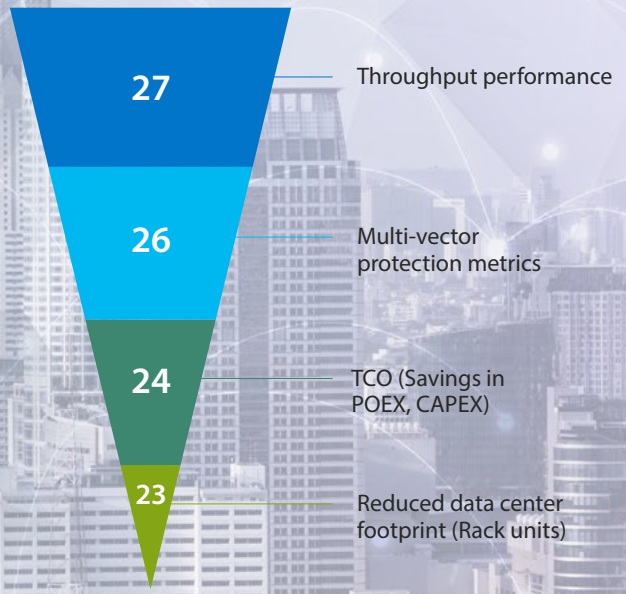
A corroborating factor is that no particular feature or capability stands out as the most important when selecting a new DDoS solution, though the number one feature, automated detection and mitigation, has increased slightly in prevalence from 18% to 24%. Impact and benefit considerations are also relatively unchanged, with respondents unwilling to say one benefit outshines the rest.

However, expectations on vendors have changed significantly since 2015. Whereas performance guarantees were seen as important by only 47% of respondents in 2015, this criterion has taken top place according to 72% of organizations surveyed. In other words, while respondent organizations want solutions to deliver across the board, they need to be trusted to cope with the current scale of attacks.

**Features and Capabilities**




**Important Benefits**

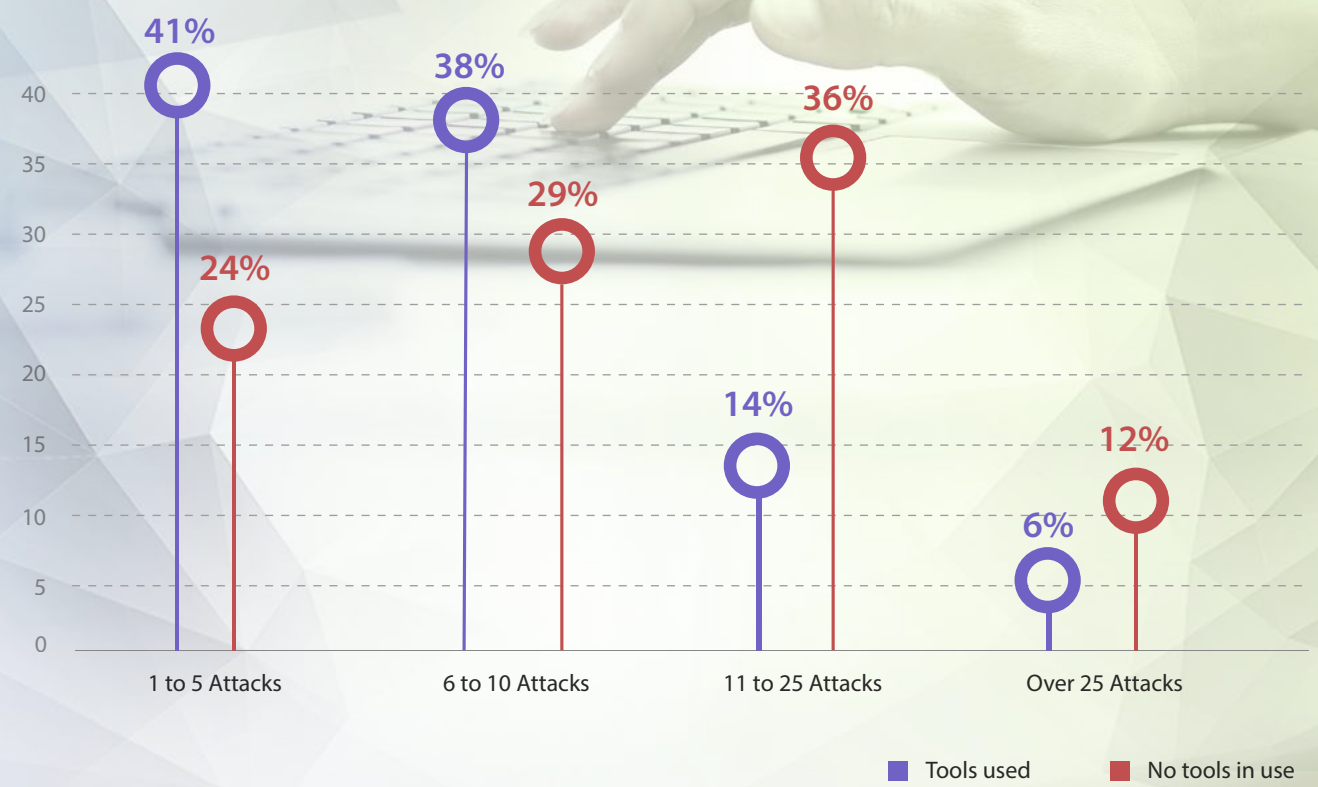



Percentage of respondents

# 04. THE GOOD NEWS: DDoS PROTECTION SOLUTIONS ARE SEEN AS EFFECTIVE

When we asked the direct question, "just how effective are DDoS protection solutions overall?" the overwhelming majority (81%) of respondents reported that they are effective in managing large-scale, multi-vector DDoS attacks. To reinforce this point, organizations with no tools in use continue to experience relatively higher numbers of attacks – 36% of this group had experienced 11 to 25 attacks, compared to 14% with tools in place.

**Number of DDoS Attacks In Past Year**



# 04. THE GOOD NEWS: DDoS PROTECTION SOLUTIONS ARE SEEN AS EFFECTIVE

The overall consequence is that over the past two years, resulting downtime has shifted from being measured in days to hours — showing the increased effectiveness of protection (plus increased experience, see below) even if an attack takes place. Only 15% of attacks result in greater than 25 hours' downtime today, compared to 29% in 2015.

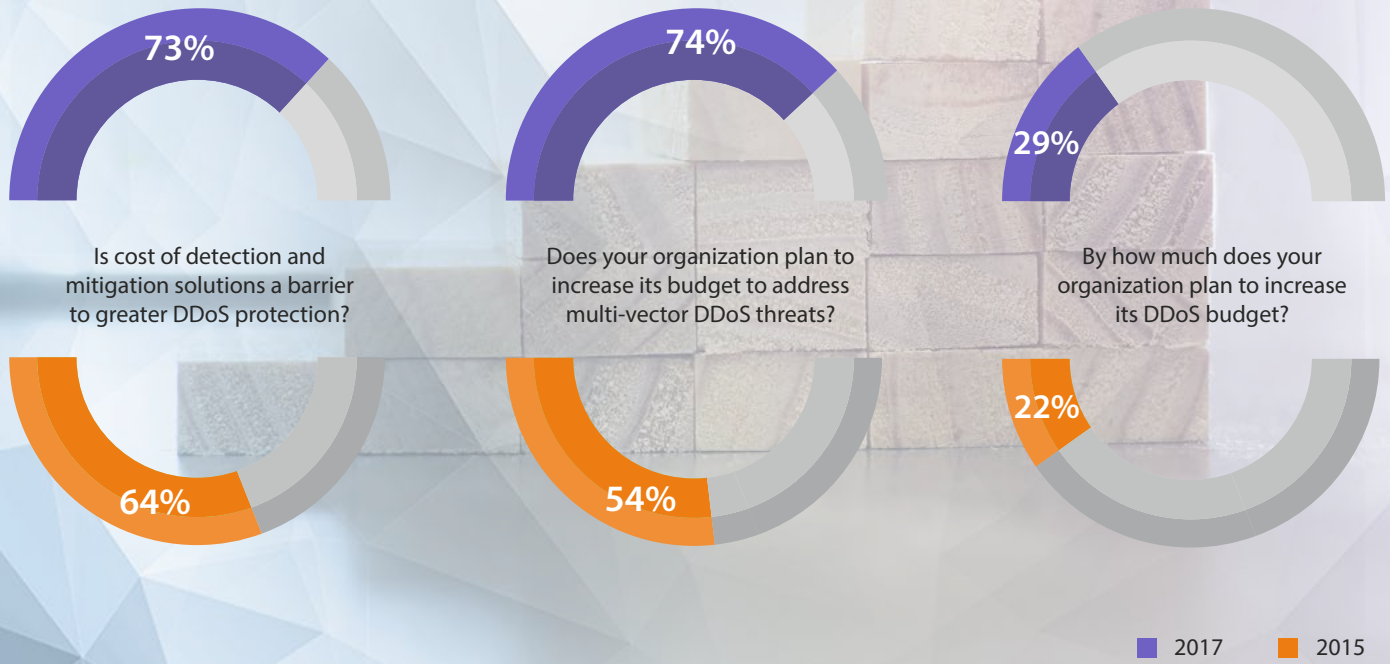
The fact that metrics have now moved toward the customer is also illustrative. Customer satisfaction is used by 86% of respondents to measure downtime impact, followed by time to service restoration and amount of time that order processing is offline (82% each). In 2015, customer satisfaction was listed at 66%.

**Average Effective Downtime Due to a DDoS Attack**


Percentage of respondents

# 05. THIS IS DRIVING FOCUS ON COST EFFECTIVENESS

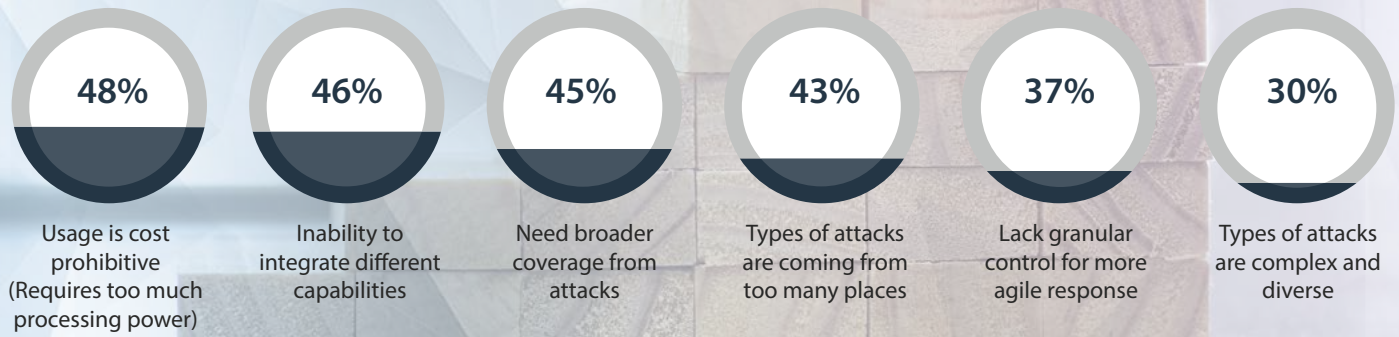
This brings to light an important insight around the cost of DDoS solutions. At first glance, it appears that cost is a growing challenge: 73% of respondents saw it as an internal barrier, compared to 64% in 2015. However, when we look at budget allocations, we see a significant proportion of organizations looking to increase their budget allocations for DDoS: 74% of respondents say budgets are increasing, compared to 54% two years ago. The amount of budget increase has also risen, from 22% to 29%. The fact that cost is increasingly seen as a barrier, yet budgets are increasing, suggests that decision makers are working harder to locate the funding required.



# 05. THIS IS DRIVING FOCUS ON COST EFFECTIVENESS

This view is reinforced if we look at the perceived limitations of DDoS solutions. Usage costs are seen as the number one issue according to 48% of respondents; bottom of the list meanwhile is attack complexity, at 30%. In other words, respondents are happier about the ability of their chosen solutions to deliver, than they are about the cost of doing so. Note also that results and impact are seen as more important than features and capabilities by 60% of respondents compared to 40%.

**Reason for Considering Changing DDoS Solution**

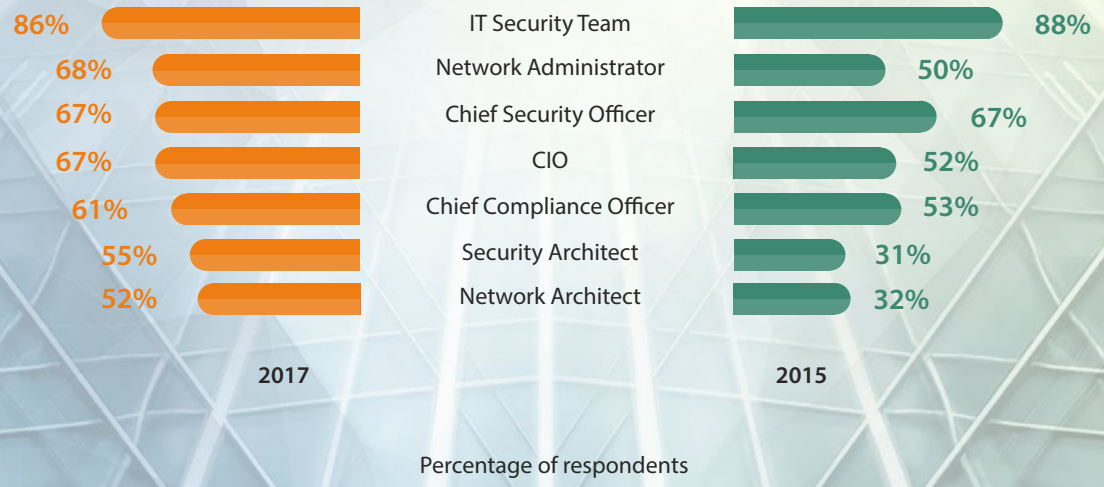



Percentage of respondents

# 06. FUTURE PROTECTION REQUIRES REVIEW OF EVOLVING BUSINESS PRIORITIES AND DDoS THREATS

A significant finding from the research is research is how the responsibility for DDoS prevention has evolved in recent years. While the IT security team still tops the list in terms of responsibility (according to 86% of respondents), multiple other roles including network administrator, security architect and network architect have increased in importance since 2015. This indicates an increase in skills and experience across across disciplines. To corroborate this, an overwhelming majority of organizations (86% selected three or more options) involve several parties in these efforts. Furthermore, insufficient expertise is seen as less of a limitation, dropping from 52% of respondents to 34% over the past two years.

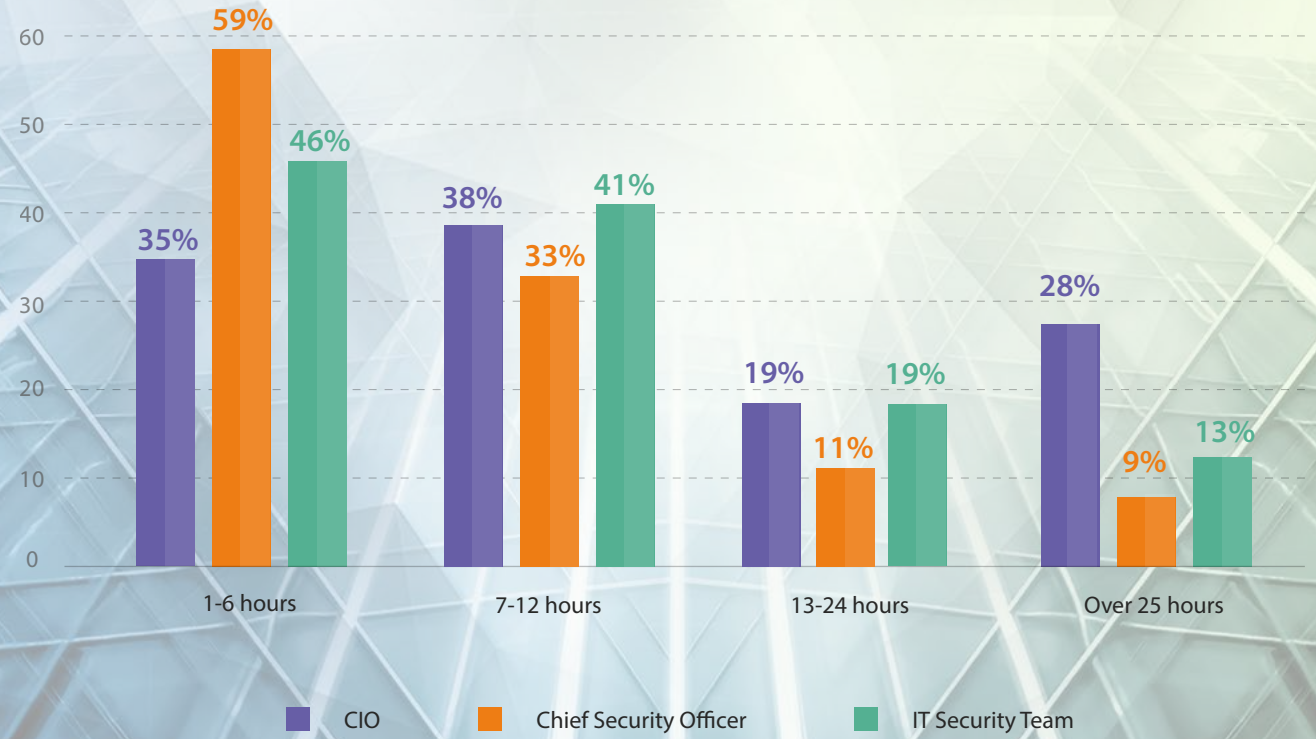
**Responsibility for Organization's DDoS Prevention Efforts**



# 06. FUTURE PROTECTION REQUIRES REVIEW OF EVOLVING BUSINESS PRIORITIES AND DDoS THREATS

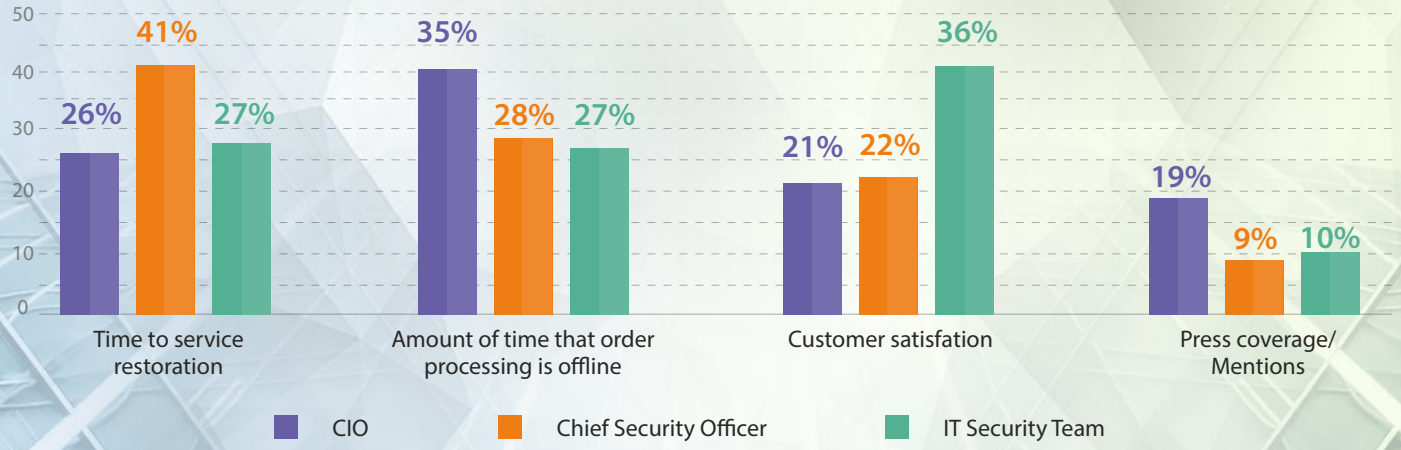
Building on the above, we can see how differences in responsibility correlate with the impact of DDoS attacks. As the figure below shows, 9% of respondent organizations with the CSO in primary responsibility saw attacks lasting longer than 25 hours, compared to 28% where the CIO had primary responsibility. However, in situations where attacks last 6 hours or less, CSO involvement is markedly negative compared to CIO involvement.

**Resultant Downtime of DDoS Attack**



# 06. FUTURE PROTECTION REQUIRES REVIEW OF EVOLVING BUSINESS PRIORITIES AND DDoS THREATS

While it is difficult to say with confidence, this could be because CSOs and CIOs have different priorities. For example, organizations with CSOs in primary responsibility see Time to Service Restoration as the most important criterion, whereas organizations with CIOs in primary responsibility see the Time Order Processing is Offline as more important. It is likely that different criteria impact DDoS attacks in different ways. This correlation is of prime importance when looking to define a DDoS solution: one organization may see customer satisfaction as the primary goal, whereas keeping the back office up and running is of secondary importance. Another organization may believe the inverse is true. Business priorities vary by organization, and by teams within those organizations.




Not only does this mean that organizations need to set business priorities for their DDoS response – are security-linked criteria more important than operational criteria, for example? - but it also sends out an important message against becoming complacent, for those organizations that already have DDoS solutions in place. As the landscape continues to change and grow, new attack vectors will emerge and DDoS attacks will continue to grow in size and complexity. This will call into question the tools already in place, along with the criteria, strategies, and expertise to deploy them.

Any DDoS strategy should therefore be subjected to frequent, rigorous review, against both changing business priorities and the evolving nature of potential threats. As skills increase against an evolving threat landscape, organizations can discern where they should spend both their time and their budgets when setting DDoS strategy and deploying the solutions that result.

# 07. ABOUT THE RESEARCH

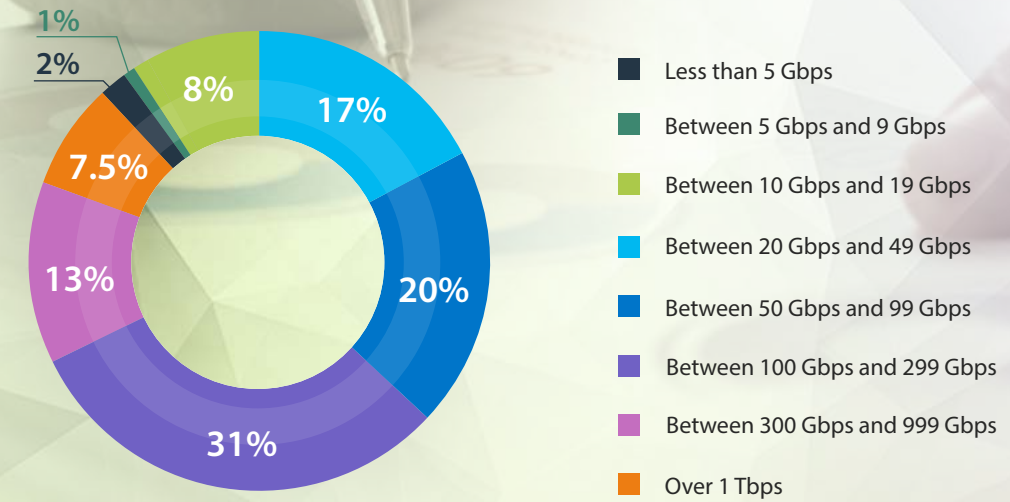
IDG Connect conducted a survey on behalf of A10 Networks to study and understand the digital security landscape. Special attention was paid to the distributed denial of service (DDoS) threats that organizations face, across industries.

IDG Connect conducted the research using an online survey with more than 200 respondents from United States and United Kingdom. Organization size was set at over 500 employees, with close to half from 1,000- to 4,999 employee organizations (41%).

**Respondent profiles were as follows:**

- All respondents were either involved in or aware of their organization's DDoS situation over the past 18 months
- Respondents came from organizations with different data center network connectivity levels; more than one in two had connectivity speeds of above 100 Gbps (51%)
- All respondents are from IT functions. The majority are decision makers; while about half are executive decision makers and one in three are technical decision makers (49% and 33% respectively)

**Network Connectivity Level Between Organization's Data Centers**




Percentage of respondents

Part Number: A10-EB-14108-EN-01 SEP 2017