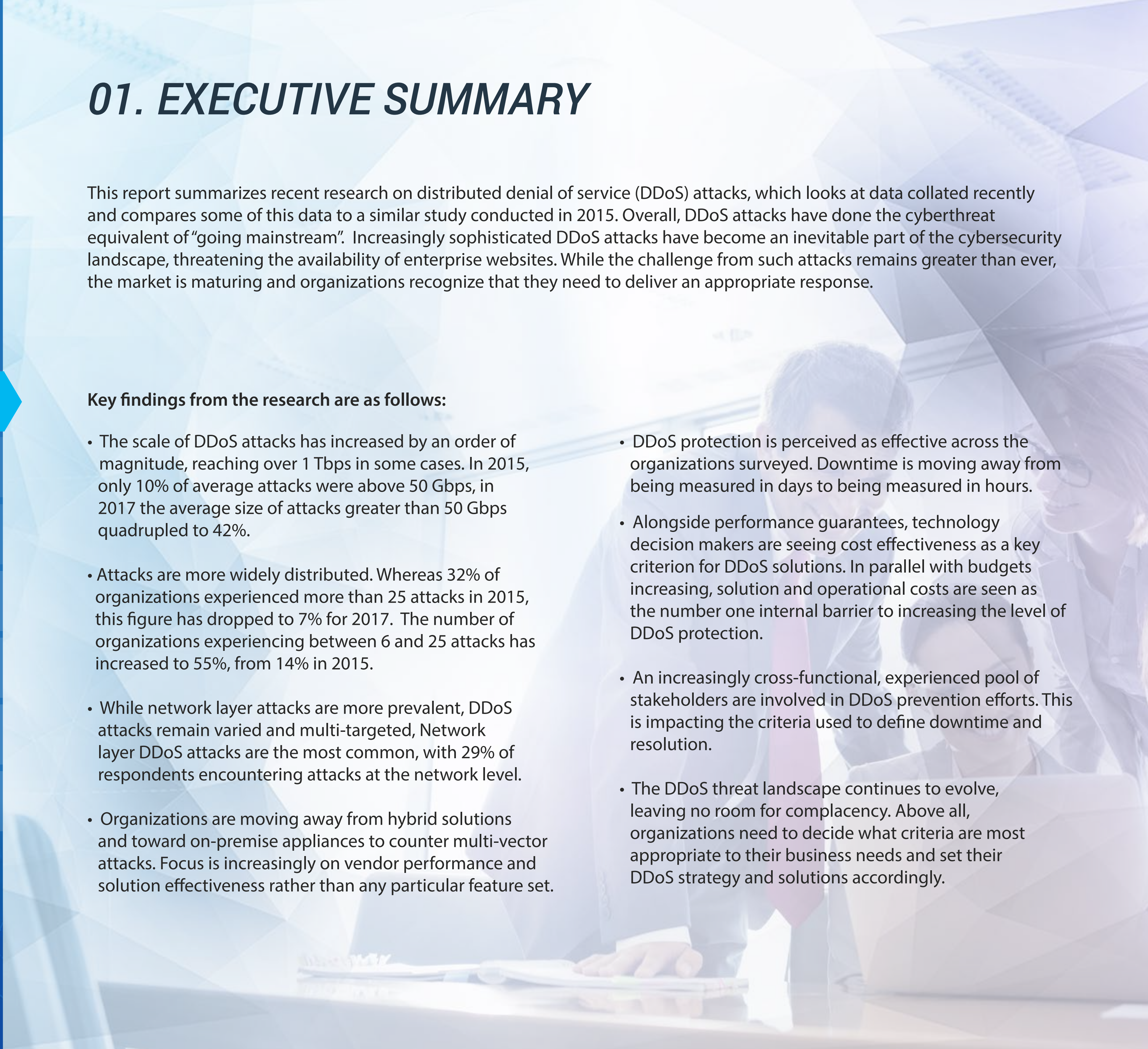
DDoS: STRATEGIES FOR DEALING WITH A GROWING THREAT

CONNECT

SUMMARY
THREATS
SOLUTIONS
EFFECTIVENESS
SPENDING
RESPONSIBILITY
ABOUT

01. EXECUTIVE SUMMARY

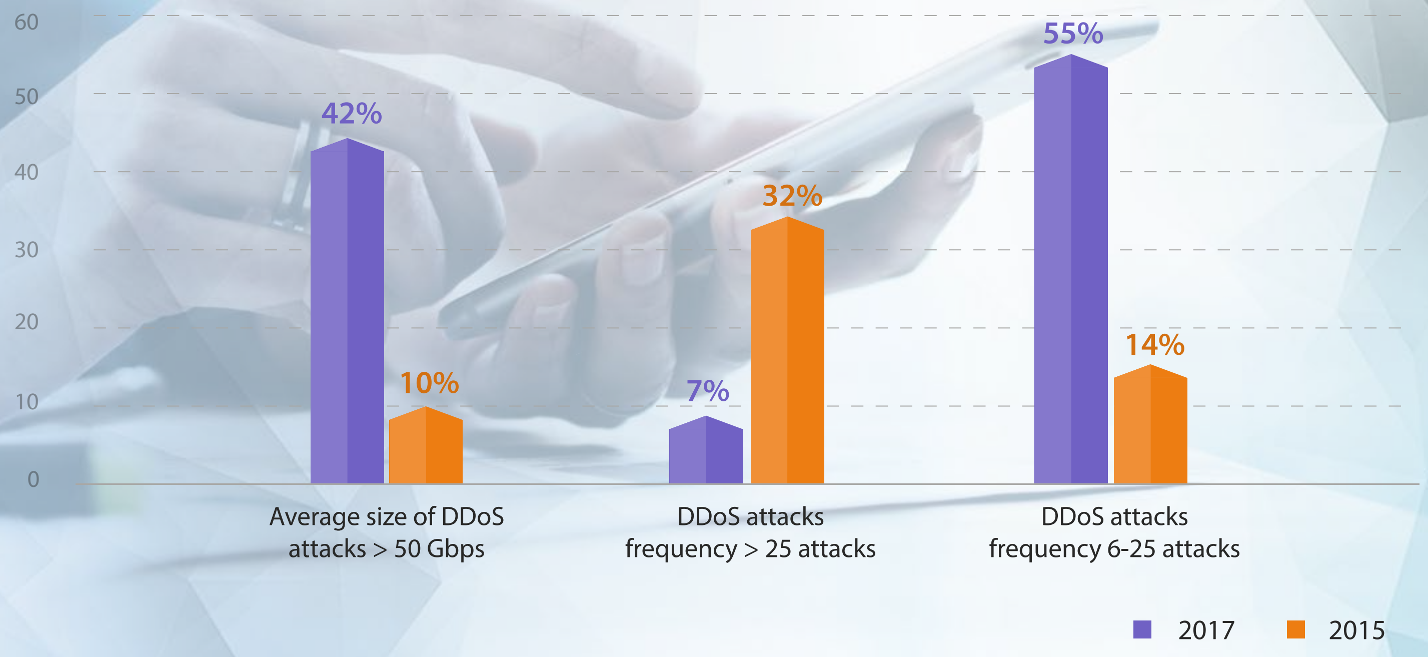


This report summarizes recent research on distributed denial of service (DDoS) attacks, which looks at data collated recently and compares some of this data to a similar study conducted in 2015. Overall, DDoS attacks have done the cyberthreat equivalent of "going mainstream". Increasingly sophisticated 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.