MAZEBOLT

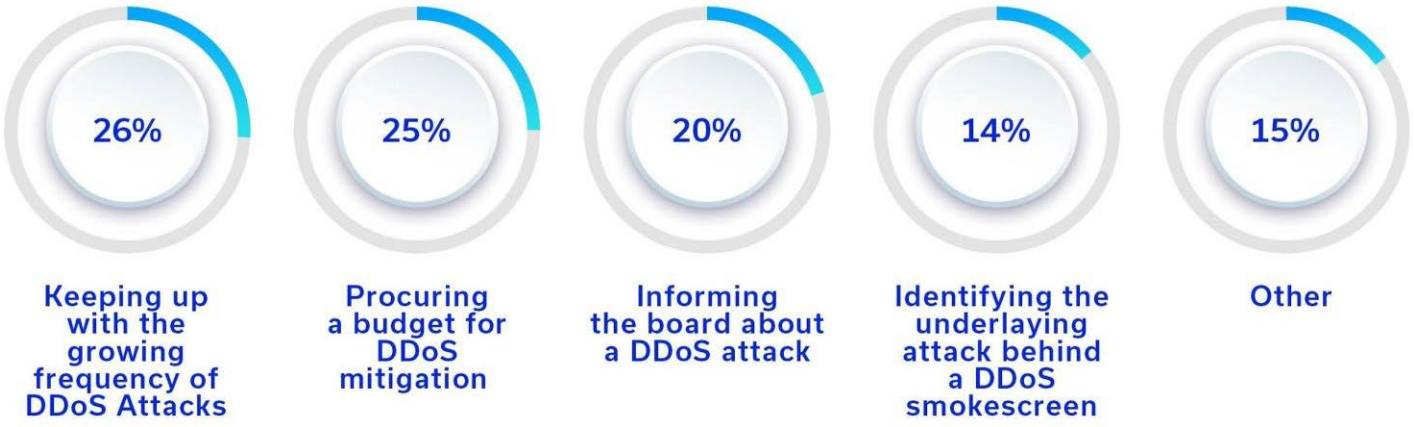
STATE OF DDOS PROTECTION 2022

CISO 2022 DDOS REPORT

KEY DDOS PRIORITIES

This report is an overview of our 2022 survey results filled in by CISO's from global enterprises. The report is industry agnostic and provides valuable insights on their current state of DDOS protection, challenges, and priorities.

1. WHAT IS YOUR TOP DDOS CHALLENGE?

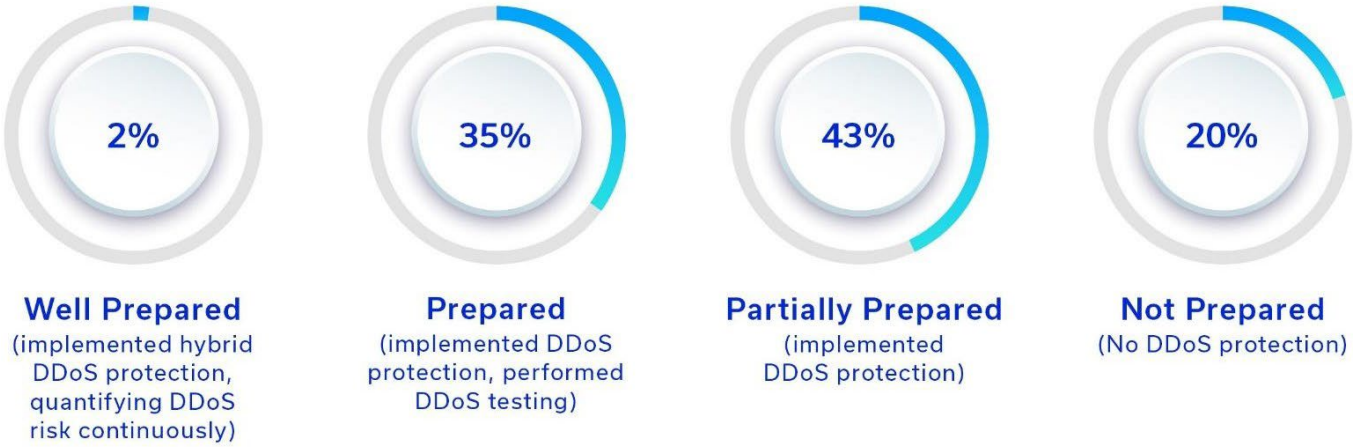


Key Takeaway: One of the major challenges is the 'growing frequency and sophistication of the current DDoS attacks which have made DDOS protection a priority for 2022. RDDOS (ransom-based) attacks have increased by more than 30% year on year and this year are expected to grow by more than 100%.

2. WHAT IS YOUR WORST CONSEQUENCE FROM A DDOS ATTACK?

Key Takeaway*:* Loss of revenue is the most immediate and visible of all side effects of a damaging DDOS attack. However, customer churn and decreased market share are longer-term damages and are often harder to repair.

3. HOW PREPARED ARE YOU FOR A DDOS ATTACK?



Key Takeaway: Only 35% of those surveyed had a DDOS mitigation solution installed along with yearly testing. However, in our experience, companies experience a staggering 48% DDOS vulnerability level even with the best mitigation solutions installed.

4. DO YOU HAVE ACCESS TO REAL-TIME REPORTS ON ONGOING NEW DDOS VULNERABILITIES?

Key Takeaway: More than half of the CISO's asked had no visibility into ongoing and new vulnerabilities in their system. To be fully protected all the time organizations need to identify vulnerabilities, reconfigure mitigation policies, and revalidate remediation continuously.

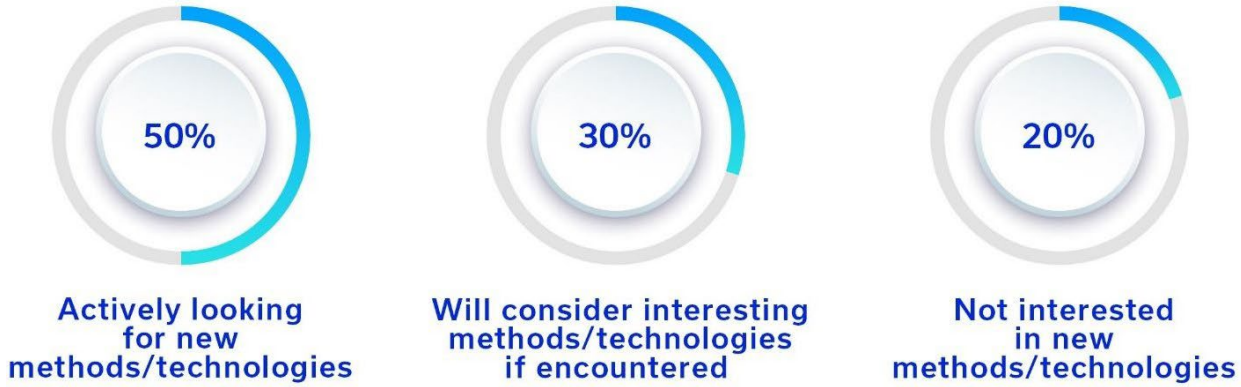
5. HOW PREPARED IS YOUR ONSITE RESPONSE TEAM TO MANAGE DDOS ATTACKS (e.g., DDOS PLAYBOOK, DDOS TESTING, ETC.)?

Key Takeaway: The CISOs who opted for well-prepared refer to their mitigation solution providers and their emergency response teams. The time taken by an emergency response team to mitigate an attack can take a minimum of 30 minutes and go on for several days, all this while the network is often down.

6. DO YOU BELIEVE YOUR CURRENT DDOS MITIGATION SOLUTION PROTECTS YOUR ENVIRONMENT FROM ALL DDOS ATTACKS?

Key Takeaway: Most CISO's asked were not confident that all DDoS attacks could be detected and stopped before damaging their business continuity. Mitigation solutions don't stop all damaging DDOS attacks. Why? Because they don't detect all DDOS attacks, as they don't constantly configure the solution to fit ongoing network changes.

7. ARE YOU CONSIDERING/SEARCHING FOR NEW METHODS OF DDOS PROTECTION SOLUTIONS IN 2022?



Key Takeaway: The majority of CISO's indicated that they would like to strengthen their defenses against DDOS attacks and are searching for new and innovative ways to better protect their network from damaging DDoS attacks.

8. DO YOU THINK CONTINUOUS AND AUTOMATED NON-DISRUPTIVE DETECTION OF DDOS VULNERABILITIES IS THE WAY TO PREVENT ATTACKS?

Key Takeaway: Overall, CISOs admitted that there were gaps in their DDOS protection process. Keen to ensure complete and ongoing protection in 2022, they are open to trying automatic detection, analysis, and prioritization of DDOS vulnerabilities across the network.

About MazeBolt

MazeBolt is pioneering a new standard in testing DDoS vulnerabilities that provides enterprises with full attack surface coverage. Its solution, RADAR™ testing, continuously observes tens of thousands of potential DDoS attack entry points, identifying how attackers succeed in bypassing existing mitigation systems. The solution's autonomous risk detection allows cybersecurity teams to go beyond traditional DDoS testing by continuously detecting, analyzing and prioritizing remediation across the network with zero operational downtime. Global enterprises, including financial services, insurance, and governments rely on MazeBolt for full visibility into their DDoS security posture. For more information visit www.mazebolt.com.