Global Distributed Denial of Service (DDoS) Protection - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Global Distributed Denial of Service Protection Market size is estimated at USD 4.15 billion in 2024, and is expected to reach USD 8.01 billion by 2029, growing at a CAGR of 14.04% during the forecast period (2024-2029).

With the emergence of the COVID-19 pandemic, working environments have shifted almost entirely to the web. People worldwide have increasingly started working, studying, and shopping online as compared to before. This has also been reflected in the goals of recent DDoS attacks, with the most targeted resources being the websites of medical organizations, delivery services, and gaming and educational platforms.

Key Highlights
-An alarming increase in the number of network attacks is anticipated to be a significant driver for the adoption of DDoS protection solutions. The threat of these attacks is driven by ready access to easy-to-use tools and a more comprehensive criminal understanding of its potential for profit through extortion. These attacks directly target business systems and individuals, which could lead to enormous financial and personal losses.
-The requirement for DDoS protection for enterprises has gained tremendous significance, as failure to deal with the attacks can affect revenue, productivity, reputation, and user loyalty. According to Cloudflare, the financial burden of a DDoS attack is significant, as falling victim to a DDoS attack can cost an organization around USD 100,000 for every hour the attack lasts, further fuelling the demand for DDoS protection solutions.
-Additionally, as per Cloudflare, DDoS attacks are surging in frequency and sophistication. After doubling from Q1 to Q2, the total number of network layer attacks witnessed in Q3 doubled again, resulting in a 4x increase compared to the pre-COVID-19 levels in the first quarter. The company also witnessed more attack vectors deployed than ever. While SYN, RST, and UDP floods continue to dominate the landscape, the company saw an explosion in protocol-specific attacks such as mDNS, Memcached, and Jenkins

DoS attacks.
-As per Cisco, the number of DDoS attacks exceeding 1 gigabit per second of traffic is expected to rise to 3.1 million by the mid-forecast period, i.e., by 2021, which is a 2.5-fold increase from 2016. In recent years, these attacks have increased in frequency and severity.
-Moreover, the United States observed the highest number of L3/4 DDoS attacks under the country-based distribution, followed by Germany and Australia. The top countries affected by region include North America (United States, Canada), Europe (Germany, Russia, among others), the Middle East (UAE, Kuwait), Asia-Pacific, and Oceania (Australia, Thailand, Japan).
-The telecom industry was at the top when DDoS attacks most targeted it during the first quarter of 2021. According to Cloudflare, application-layer attacks are on the rise, and those that aim to disrupt the HTTP server's ability to process requests are reasons for significant concern. Also, ransom DDoS attacks continued to be a significant challenge during the first quarter of 2021.

Distributed Denial of Service (DDoS) Protection Market Trends

Increasing Instances of Sophisticated DDoS Attacks to Drive the Market

- The rapidly rising instances of DDoS attacks across multiple industries, which have disrupted crucial organizational services and the loss of millions of dollars for various companies, have increased the focus on robust protection solutions across emerging economies.
- Network layer attacks that target exposed network infrastructure such as inline routers and other network servers significantly impact data centers where a significant share of IT and telecom vendors operate. According to Cloudflare, about 44% of network layer attacks occurred in January 2021, with synchronizing flag (SYN) packet flood attacks remaining the most common. Other attacks noted included reset flag (RST) packets, user datagram protocol (UDP), and domain name system amplification attacks. Due to such developments, DDoS protection is vital for vendors operating in these industries.
- The increased bandwidth and low latency in 5G are further anticipated to increase the volume and severity of the attacks. According to Corero's study, the higher bandwidth of 5G enables advanced botnets to harness as many mobiles or IoT devices as possible to cripple their targets.
- Further, with the adoption of remote working due to the onset of Covid, corporate networks have become more vulnerable when accessed from unsecured work-from-home environments, as personal computing devices are not always protected, thus causing an increase in Botnet DDoS attacks.
- As businesses worldwide grow, new and advanced persistent threats have exposed critical services to risk. This has encouraged organizations to deploy better DDoS solutions to safeguard their endpoints and networks against potential attacks.

North America is Expected to Hold a Major Share

- The North American region is expected to hold a significant market share, primarily due to the higher adoption of advanced technologies and stricter implementation of cybersecurity solutions. Given the need to meet stringent regulatory and compliance requirements, there is a rising need for advanced security systems among the region's end-user industries that positively boost the market's growth.
- The region also accounts for a significant number of DDoS attacks, which are likely to increase with respect to multiple end-user industries, further driving the demand for DDoS protection solutions. Moreover, cyberattacks in the region, especially in the United States, are increasing rapidly. They are reaching high numbers, primarily owing to the rapidly increasing number of connected devices in the region.
- Also, in the United States, consumers have been using public clouds, and multiple mobile applications are preloaded with

personal information for the convenience of banking, shopping, and communication. In the past few years, companies in the region have been witnessing increasing DDoS attacks, which has resulted in tremendous awareness related to protection solutions. Also, according to the White House Council of Economic Advisers, the US economy loses approximately USD 57 billion to USD 109 billion per year to harmful cyber activity.
- Moreover, according to Atlas VPN, it was estimated that there were more than 175,000 DDoS attacks in the United States in March 2020 alone. Attackers tried to disable the website of the US Department of Health and Human Services. The primary purpose seemed to deprive the citizens of access to official data regarding the COVID-19 pandemic and the measures being taken against it.
- The US government also signed a law to establish the Cybersecurity and Infrastructure Security Agency (CISA) to enhance the national defense against cyberattacks. The agency works with the federal government to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard the governmental networks that support essential operations of the partner departments and agencies. As a result, it opens new avenues for the new and existing companies to invest in a suitable protection suite designed for the industry.
- Various firms are deploying standalone 5G networks, and they would need security partners to become ingrained in their network and security against attacks well before a threat occurs. For instance, in April 2021, DISH Network Corporation chose Allot Ltd to provide end-to-end User Plane Protection (UPP) against DDoS and botnet attacks on the United States' cloud-native, OpenRAN-based 5G network.

Distributed Denial of Service (DDoS) Protection Industry Overview

The DDoS protection market primarily comprises multiple domestic and international players fighting for attention in a somewhat contested market space. The market is also characterized by growing product penetration, moderate/high product differentiation, and high levels of competition. The market is product-centric, and technological advancements constantly govern it. Innovations, R&D investments, partnerships, and M&As are expected to be part of the competitive strategy among the vendors operating in the market. Overall, the intensity of the competitive rivalry is high, and it is expected to remain the same during the forecast period.

- June 2022 - G-Core Labs, in partnership with Intel, launched a standalone solution (eBPF) providing mitigation of DDoS attacks with a low impact on overall latency. The XDP-based solution removes the need for a dedicated DDoS protection server role and protects against SYN Flood DDoS attacks.
- March 2022 - Corero Network Security, a real-time, high-performance DDoS cyber defense solutions provider, extended its automatic protection against Botnet and Carpet Bomb attacks. The company's mission is to make the internet a safer place to do business by protecting against the disruption and downtime caused by DDoS attacks.
- February 2022 - Radware acquired SecurityDAM for USD 30 million, with contingent payments of up to USD 12.5 million for Radware's cloud DDoS protection service after the deal.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Global Distributed Denial of Service (DDoS) Protection - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-27
		Signature