Deep Packet Inspection and Processing - 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 Deep Packet Inspection and Processing Market size is estimated at USD 28.17 billion in 2024, and is expected to reach USD 71.01 billion by 2029, growing at a CAGR of 20.32% during the forecast period (2024-2029).

DPI combines signature matching technology with a data analysis algorithm to determine a communication stream impact. Hardware-based middleboxes are prevalent in computer networks, which usually incur high deployment and management expenses.

Key Highlights
-A recent trend addresses those problems where researchers propose two practical approaches to implement a cloud-based DPI middlebox. The outsourced DPI middlebox performs payload inspection over encrypted traffic while preserving the privacy of both communication data and inspection rules.
-The proliferation of technologies, such as cloud deployment, remote working, BYOD, SaaS applications, etc., are increasing the paths available to cyberattacks. Applications have become inviting targets for cybercriminals, but securing, protecting, and controlling the networks that connect them is a huge challenge for network security providers.
-In contrast, DPI in the European Union is used very differently. It is used as part of mechanisms to clamp down on drug trafficking and child pornography. When the EU established its intent, they were quick to enforce laws that controlled the use of data. The consideration falls under the General Data Protection Regulation (GDPR), a comprehensive set of laws protecting EU citizens and their sensitive data.
-With the growing global IP traffic augmented by mobile devices, the emergence of the Internet of Things (IoT) and cloud computing require close attention and powerful tools to ensure secure operations on an enterprise network. According to CISCO Systems, the global IP data traffic is expected to reach 278,108 petabytes per month by 2021.

-Many cloud services are accessible to the entire internet, which means improved system accessibility is an important driver for cloud migrations. However, cloud servers and applications are regularly attacked using various methods from anywhere globally. Deep packet inspection and processing are essential to keep the bad traffic out while letting the good traffic through without too much interruption. It is also important to look beyond this perimeter-based defense layer. There are several approaches to successfully deploying a security control based on Deep Packet Inspection within a public cloud environment, such as using the vendor solutions already built for this exact purpose, and another product range is based on agents running on customer endpoints.
-Moreover, attackers started exploiting the burst of information and heightened public alertness for COVID-19-related news. Phishing, spam campaigns, and malicious websites/domains significantly increased. To relieve the load on VPNs and mitigate the chances of successful command and control (C2) channels for malware to be established, F-Secure recommends using deep packet inspection on VPN concentrators and other network perimeter devices. Certain bandwidth-heavy online services, such as streaming and various gaming services, can be blocked with such a stand. It is also recommended to allow communication on only known and approved ports, such as HTTPS. The pandemic is significantly increasing the adoption rate.

Deep Packet Inspection and Processing Market Trends

Software Solution to Witness Significant Growth With Increasing Enterprise Internet Traffic

- In recent years, DPI (Deep Packet Inspection) software has evolved into a powerful tool to meet new network challenges, playing a central role in today's internet and network infrastructure. As most internet traffic is now encrypted, a reliable DPI software engine needs a tool kit of advanced techniques to classify traffic.
- DPI identifies and classifies traffic based on the signature database that includes information extracted from the data part of a packet, allowing finer control than classification based only on header information. Applications such as peer-to-peer (P2P) traffic provide increasing problems for broadband service providers.
- Typically, P2P traffic is used by applications providing file sharing. Due to its frequently large size of media files being transferred, P2P drives the increasing traffic loads, which requires additional network capacity. DPI allows operators to oversell their available bandwidth while ensuring equitable bandwidth distribution to all users by preventing network congestion.
- The network must be able to parse through content, assemble enough of an application message, and identify traffic usage and patterns based on the information. DPI functions fall into four categories: Protocol analysis/application recognition, Anti-malware/anti-virus, Intrusion Detection and Prevention (IDS/IPS), and URL filtering.
- According to the Enea AB survey, 70 percent of respondents (high-tech product managers) require the classification of connected devices in the enterprise and IoT/industrial networks. And also, the increased use of encryption and the adoption of the stringent TLS 1.3 security protocol (mandatory in 5G) threatens essential traffic visibility for many vendors. This requires Deep packet inspection and processing catering to future market growth.
- Further, most vendors report that they have or are developing cloud solutions, with half planning to offer a Secure Access Service Edge (SASE) solution that integrates security and networking in a cloud-based service. This requires the use of DPI software, which adheres to market growth.

North America Accounts for the Significant Market Share

- North American accounts hold a significant share as the region's growth is driven by the rising internet penetration and increasing adoption of cloud-based and IoT applications across verticals. Moreover, North America tops the world regarding security breach incidents, which caters to DPI adoption.

- Cybercriminals increasingly target businesses and medical institutions to gain the victim's data. The personal data is then often used for socially engineering their attacks, which are more likely to trick the victim when compared to traditional cyber attacks. 79% of the total data breaches recorded in the United States were reported in the business and medical sectors (source: Identity Theft Resource Center).
- The HIPAA Privacy Rule established national standards to safeguard Protected Health Information (PHI), individual medical records, and other personal health information. This is following the trend towards deploying servers executing sophisticated Deep Packet Inspection (DPI) logic to identify and extract relevant data segments from the raw traffic.
- By countries data breaches in the United States continued to be more expensive than those in other nations. Data breaches in the country, on average, cost USD 8.64 million, which is nearly double that of the global average, and this increased by over 130% over the last 14 years.
- This DPI technology, available for macOS and embedded into the Endpoint Protector client, intercepts all file transfers through web browsers. With such a feature now, it is possible to monitor a file's destination and whitelist and blacklist specific URLs. Whitelisting allows file transfers only to specific domains and URLs, while with the blacklisting option, access to specific websites can be blocked.

Deep Packet Inspection and Processing Industry Overview

The deep packet inspection and processing market is fragmented as the players are increasingly innovating new hardware and software solutions, and also new entrants are adding to this market that caters to the significant competition. Several innovations have been witnessed in the deep packet inspection and processing market, including developing Next-Generation Firewalls (NGFWs) that can investigate the network packets up to 7 application layers of the OSI model. Such instances provide intense rivalry among the players to provide unique solutions. Nokia (Alcatel Lucent), SolarWinds Worldwide, LLC, cisco systems, and Huawei Technologies are key players. Recent developments in the market are -

In February 2023, Cisco announced plans to purchase Lightspin, an Israeli cloud security business. Cisco and Lightspin will be able to achieve their mutual goal of assisting customers in modernizing their cloud infrastructures by providing end-to-end security and observability from construction to runtime.

In August 2022, SafeRide Technologies announced the release of new Intrusion Detection and Prevention Software (IDPS) to protect Automotive Ethernet networks against cyberattacks. The new solution was integrated into SafeRide's vSentry Edge AI software. vSentry Edge AI monitored the CAN and Ethernet communications from multiple domains, performing deep packet inspection and payload analysis.

Additional Benefits:

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

Table of Contents:

1 INTRODUCTION
1.1 Study Assumptions and Market Definition
1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET DYNAMICS
4.1 Market Overview
4.2 Industry Value Chain Analysis
4.3 Industry Attractiveness - Porter's Five Forces Analysis
4.3.1 Bargaining Power of Buyers/Consumers
4.3.2 Bargaining Power of Suppliers
4.3.3 Threat of New Entrants
4.3.4 Threat of Substitute Products
4.3.5 Intensity of Competitive Rivalry
4.4 Regulatory Implications
4.5 Assessment of COVID-19 Impact on the Market
4.6 Market Drivers
4.6.1 Increasing Adoption of Regulatory and Data Protection Laws
4.6.2 High Adoption of Cloud Based Security Technologies
4.7 Market Restraints
4.7.1 DPI Adds to the Complexity and Unwieldy Nature of Existing Firewalls and Other Security-Related Software

5 MARKET SEGMENTATION
5.1 Solution
5.1.1 Hardware
5.1.2 Software
5.2 Deployment
5.2.1 On-Premise
5.2.2 Cloud
5.3 End-User
5.3.1 Telecom and IT
5.3.2 BFSI
5.3.3 Healthcare
5.3.4 Retail
5.3.5 Other End-Users
5.4 Geography
5.4.1 North America
5.4.1.1 United States
5.4.1.2 Canada
5.4.2 Europe
5.4.2.1 Germany
5.4.2.2 United Kingdom
5.4.2.3 France
5.4.2.4 Rest of Europe
5.4.3 Asia-Pacific
5.4.3.1 China
5.4.3.2 Japan
5.4.3.3 Australia
5.4.3.4 Rest of Asia-Pacific
5.4.4 Latin America
5.4.5 Middle East and Africa

6 COMPETITIVE LANDSCAPE
6.1 Company Profiles
6.1.1 Nokia Corporation (Alcatel Lucent)
6.1.2 Allot Ltd.
6.1.3 Bivio Networks, Inc.
6.1.4 Huawei Technologies Co., Ltd.
6.1.5 Enea AB (Qosmos SA)
6.1.6 WiseSpot Company Limited
6.1.7 SolarWinds Worldwide, LLC.
6.1.8 NetFort Technologies Limited (Rapid7
6.1.9 Netify
6.1.10 AppNeta, Inc.
6.1.11 ManageEngine (Zoho Corporation)
6.1.12 Cisco Systems, Inc.
6.1.13 ipoque GmbH

7 INVESTMENT ANALYSIS

8 MARKET OPPORTUNITIES AND FUTURE TRENDS

Deep Packet Inspection and Processing - 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	2026-03-04
		Signature