Market Publishers

Adaptive Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

https://marketpublishers.com/r/ACAA37581F3EEN.html

Date: July 2024
Pages: 119
Price: US$ 4,750.00 (Single User License)
ID: ACAA37581F3EEN

Abstracts

The Adaptive Security Market size is estimated at USD 12.28 billion in 2024, and is expected to reach USD 27.92 billion by 2029, growing at a CAGR of 17.86% during the forecast period (2024-2029).

Key Highlights

A significant factor driving the demand growth is that firms are constantly being attacked by progressive threats such as advanced persistent threats, zero-day malware, and different targeted attacks. Dynamic and orchestrated, these modern cyberattacks seek to exploit weaknesses in an organization's traditional defenses.

Enterprises have been adopting prevention strategies to increasingly keep track of such undetectable threats to protect the organizations' data, networks, and applications. The growing need for security compliances and regulations and the need to secure IT resources from sophisticated and complex cyberattacks are major factors expected to drive the adaptive security market over the forecast period.

Law firm DLA Piper states that since the Europe-wide implementation of the General Data Protection Regulation (GDPR) in May 2018, the highest number of personal data breaches as of January 2023 were reported in the Netherlands, a total of around 117,434. Germany ranked second, with more than 76,000 private data breach notifications. Such a massive rise in data breaches is propelling the demand for the market.

In addition, the advent of 5G is expected to expedite the use of connected devices in industries already pushing toward Industrial Revolution 4.0. This revolution has aided

cellular connectivity throughout the industry through the rise of IoT. Machine-to-machine connections are driving the traction of application security.

Adaptive security solutions primarily need specialized expertise to be implemented effectively. Due to the lack of skilled cybersecurity professionals, organizations struggle to configure and deploy these solutions properly, limiting their effectiveness in mitigating threats and vulnerabilities.

With the outbreak of COVID-19, most of the organization shifted to the work-from-home model due to the lockdown and social distancing measures that created a significant demand to manage and monitor applications remotely. As a result of the rising demand from organizations for adaptive security for their application services, the need for them increased.

Adaptive Security Market Trends

Cloud Deployment Model to Witness Major Growth

The growing adoption of cloud services has necessitated the emergence of adaptive cloud security solutions, which dynamically adjust and respond to evolving threats and offer security.

Cloud-based adaptive security solutions help seamlessly integrate with any cloud service providers, enabling organizations to leverage their existing cloud infrastructure while enhancing security capabilities and driving the adoption of cloud-based adaptive security solutions by organizations across industries.

The increasing migration of workloads and data by businesses to the cloud for scalability and cost-effectiveness creates a growing need for security solutions designed to protect cloud environments. As traditional on-premises solutions are not suited to the dynamic and distributed nature of cloud infrastructure, the demand for cloud-based adaptive security solutions and services is increasing.

For instance, according to a survey of 627 technical professionals across a cross-section of organizations globally by Flexera Software, as of 2023, 50% of enterprises already had workloads in the public cloud, with 7% planning to move additional workloads to the cloud in the next 12 months. In addition, 48% of the respondents reported having data stored on the public cloud.

By end-user industry, the BFSI segment is expected to drive demand for cloud-based adaptive security solutions and services. As the BFSI industry is increasingly adopting cloud platforms, accessing industry-specific attributes related to security and compliance requirements is driving the need for adaptive security solutions to enable security. Thus, the need to match the complexities of operations and multi-faceted regulatory demands with the right cloud platform businesses in the industry is driving the need for adaptive security solutions and services in applications such as cloud security.

The market vendors are introducing cloud-based adaptive security solutions and offering automated and tailored protection. For instance, in July 2023, Egress started offering a cloud email security platform to apply an adaptive security model. With the launch of this solution, the company would offer dynamic and automated protection against advanced inbound and outbound threats, transforming how organizations manage human risk via email.

The demand for cloud-based adaptive security is growing due to the increasing adoption of cloud computing, the complexity of hybrid and multi-cloud environments, and the integration with cloud-native technologies. Implementing cloud technology across industries is anticipated to create demand for cloud-based adaptive security over the forecast period.

North America to Hold Significant Market Share

The rising need for various security solutions, including network, endpoint, application, and cloud security, drives adaptive security adoption in North America. The region's focus on improving cybersecurity to address changing cyber threats and the requirement for advanced security technologies to safeguard critical data and systems are key factors driving the adaptive security solutions market. Furthermore, factors such as the growing reliance on digital technologies, the surge in cyberattacks, and the necessity for regulatory compliance all contribute to the rising implementation of adaptive security in North America.

The United States has invested significantly in cybersecurity research and development. For instance, in August 2023, the United States Department of Energy (DOE) opened USD 9 million in competitive federal funding for small and rural electric utilities to improve cybersecurity. This will allow smaller and rural utilities and cooperatives in the

electric sector to apply for chunks of funding to build more cyber resilience in their infrastructure that could defend against cyberattacks, ransomware, and other digital threats.

Moreover, cybercrime is rapidly gaining traction in Canada, and its impact is increasing. In August 2023, the Communications Security Establishment (CSE) released a report detailing 70,878 cyber fraud cases in Canada, resulting in over USD 390 million being stolen. Organizations in Canada are investing in cybersecurity solutions to guard against emerging threats due to the mounting frequency and sophistication of cyber threats, such as ransomware attacks and data breaches.

In January 2024, Oleria, a company providing adaptive and autonomous identity security solutions, raised USD 33 million in a Series A funding round. This latest investment, which brings the company's total funding to more than USD 40 million, is led by Evolution Equity Partners with participation from Salesforce Ventures, Tapestry VC, and Zscaler. This funding round allows Oleria to ramp up hiring to enhance its overall product innovation, involving AI capabilities and its go-to-market strategy.

Overall, increased public awareness of cybersecurity risks and the potential consequences of cyber threats has contributed to a greater emphasis on implementing effective cybersecurity measures. The combination of these factors underscores the critical importance of cybersecurity in North America, leading to a growing demand for advanced solutions and proactive cybersecurity strategies across industries, driving the market's growth opportunities significantly.

Adaptive Security Industry Overview

The adaptive security market is highly fragmented due to the presence of both global players and small and medium-sized enterprises. Some of the major players in the market are Cisco Systems Inc., Trend Micro Incorporated., Rapid7 Inc., IBM Corporation, and Juniper Networks Inc. Players in the market are adopting approaches such as partnerships and acquisitions to enhance their solutions offerings and gain sustainable competitive advantage.

In November 2023, Trellix launched its generative Artificial Intelligence (GenAI) capabilities, built on Amazon Bedrock and mainly supported by Trellix Advanced Research Center. By expanding its partnership with AWS, Trellix continues investing in

GenAI to deliver enhanced threat remediation and improved customer support.

In November 2023, Trend Micro launched its new generative AI tool, Trend Companion, mainly built to empower security analysts by driving efficient workflows and enhanced productivity.

Additional Benefits:

The market estimate (ME) sheet in Excel format

3 months of analyst support

Contents

1 INTRODUCTION

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHT

5 MARKET DYNAMICS

6 MARKET SEGMENTATION

I would like to order

Product name: Adaptive Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

Product link: https://marketpublishers.com/r/ACAA37581F3EEN.html

Price: US$ 4,750.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/ACAA37581F3EEN.html