Adaptive Security - 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 Adaptive Security Market size is estimated at USD 10.77 billion in 2024, and is expected to reach USD 23.42 billion by 2029, growing at a CAGR of 16.81% during the forecast period (2024-2029).

To secure businesses' data, networks, and applications, enterprises have increasingly used preventative measures to keep track of undetected risks.

Key Highlights
-The primary factor driving adaptive security market expansion is that enterprises are continually being attacked by sophisticated threats such as advanced persistent threats (APTs), zero-day malware, and other targeted assaults. These current assaults are dynamic and coordinated, intending to exploit flaws in an organization's traditional defenses. Cybercriminals can breach a company's information technology (IT) infrastructure and access business-critical information to inflict harm and enormous financial and data loss. Protecting against increasingly sophisticated cyberattacks, then, necessitates preparation that goes beyond traditional defenses.
-Growing demand for multilayer security and smart solutions, as well as the urgent requirement for regulatory compliance, are some factors predicted to fuel market growth during the forecast period. The adaptive security market is driven by the growing usage of cloud-based security systems, particularly in organizations. However, factors such as a lack of technical skills and problems processing vast volumes of data limit the need for global adaptive security.
-Furthermore, the rising acceptance of cloud-based security solutions will likely generate attractive market development possibilities. Adaptive security strategies attempt to use an organization's present security infrastructure to develop a strong security posture. To safeguard their networks, endpoints, data, and users from malicious assaults, large and small companies (SMBs) try to deploy security solutions that can adapt to emerging threats. Businesses do not want to spend money on security

services that are not necessary.
-Prioritizing the risks most important to their business can help them learn how to prevent such assaults in the future. The industry of adaptive security faces substantial obstacles from the expanding data and the demand for more qualified employees. These barriers make it difficult for enterprises to implement adaptive security solutions. During the forecast period, the need for more seasoned cybersecurity experts is anticipated to restrain the growth of the Adaptive Security Market.
-With the outbreak of COVID-19, almost the majority of the organization shifted to the work-from-home model due to the lockdown ad social distancing measures that created a significant demand for managing the application and monitoring the application aspect remotely. As a result of the rising demand from organizations for adaptive security for their application services needs, some companies providing adaptive application security services are making strategic inroads into delivering a package of services.
-For example, OpsRamp recently expanded its network, UC monitoring for the WFH world with new functionality in the OpsRamp platform that allows solution providers to help customers manage hybrid and multi-cloud IT environments and meet the needs of work-from-home employees as demand for cloud applications, unified communications (UC) and collaboration tools, video conferencing, and other IT resources increased significantly.
-Furthermore, there was an increase in cyber-attacks and data breaches throughout the epidemic. According to VMware's Cybersecurity Threat Survey Report, supplemented with a survey on the impact COVID-19 had on the attack landscape, 88% of US cybersecurity professionals stated that as more workers work from home, attack volumes rose. Moreover, 89% reported cyberattacks tied to COVID-19 malware in their companies. Approximately 89% reported being targeted by COVID-19-related malware.

Adaptive Security Market Trends

Cloud to Hold Significant Share

- Cloud security is less expensive to install than traditional premise-based systems, and firms may save money and staff. The provider also supplies the bandwidth, IT professionals, and infrastructure to safeguard the data.
- Due to enhanced agility, cheaper capital costs, and streamlined operation (from software to infrastructure-as-a-service), businesses' rapid adoption of cloud solutions and services by enterprises need equally dynamic cloud protection. This new environment necessitates cloud-based adaptive security.
- The latency, delays, and hazards of running confidential data from a cloud provider are at risk as cyber assaults get more complicated.
- As a result, enterprises are looking to install a hybrid solution in which on-premise solutions automatically update and secure network protection regularly and utilize the cloud to give a second layer of defense against various assaults.

North America to Hold Major Share

- North America is the most active and committed area regarding cybersecurity activities. The main nations' GCI (global cybersecurity index) scores (United States of America - 100 and Canada - 97.67) reaffirm their commitment to constructing a strong cybersecurity framework.
- However, due to the existence of vital corporations and data centers, North America is rated the most susceptible. The US Department of Homeland Security identified more than 60 organizations in critical infrastructure in the United States that were damaged by a single event that cost over USD 50 billion.
- The region's SMEs (about 97% of total firms) favor cloud deployment to reduce the total cost of ownership of security solutions.

As a consequence, security solution providers have a chance to design solutions that meet customer needs. It is also predicted that most of these players would use technology and deploy effective end-point security measures to improve the client experience.

Adaptive Security Industry Overview

The adaptive security market is moderately competitive. The players in the market are innovating in providing strategic solutions to increase their market presence and customer base. This enables them to secure new contracts and tap new markets.

In March 2023, Rapid7, a cloud risk and threat detection company, announced the acquisition of Minerva Labs, Ltd., a provider of anti-evasion and ransomware protection technologies. Rapid7's Managed Detection and Response (MDR) services now give clients enhanced detection and response capabilities across cloud, on-premise, and extended attack surfaces. Rapid7's superior managed threat detection capabilities will be expanded with the ability to organize sophisticated ransomware protection due to this purchase. These new capabilities will allow companies to further consolidate their security expenditures by seamlessly extending MDR across cloud resources, legacy infrastructure, and current endpoint protection architecture.

In June 2022, Cisco, the business networking and security company, announced plans for a worldwide, cloud-delivered, integrated platform that secures and connects enterprises of any size and shape. With no public cloud lock-in, the Cisco Security Cloud was intended to be the most open platform in the market, preserving the integrity of the whole IT ecosystem.

The Security Cloud offers a unified experience for securely connecting people and devices to apps and data everywhere. The open platform delivers threat prevention, detection, response, and remediation capabilities at scale through a unified administration. Cisco has been on the path to the Security Cloud for some time and is now sharing further progress with new security advancements throughout its portfolio.

In July 2021, Rapid7, Inc., a provider of security analytics and automation, announced the release of InsightCloudSec, the fully integrated Cloud-Native Security Platform (CNSP). With continuous security and compliance for complex cloud environments, InsightCloudSec enabled organizations to improve their cloud security programs. InsightCloudSec, the newest component of Rapid7's Insight Platform, combined the cloud security posture management, infrastructure entitlements management, and infrastructure as code capabilities of DivvyCloud (acquired in May 2020), Kubernetes security provider Alcide (acquired in January 2021), and other cloud security providers into a single seamless cloud security solution.

Additional Benefits:

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

Table of Contents:

SCOTTS INTERNATIONAL

Adaptive Security - 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	

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com