

Software Defined Security Market Size Expected to Reach New Heights | Exceeding USD 68.83 Billion by 2030 at 29.5% CAGR

The market for software defined security is expanding as a result of rising need for more agile, scalable and improved security solutions.

PORTLAND, PORTLAND, OR, UNITED STATES, May 14, 2023

/EINPresswire.com/ -- The size of the global software defined security market was estimated at \$5.3 billion in 2020 and is expected to grow at a CAGR of 29.5% from 2021 to 2030 to reach \$68.83 billion.



Network latency affects whether an attack can be detected and averted, and higher network latencies may allow hostile packets to bypass security firewalls or intrusion detection systems without setting off an alarm. Software defined security services significantly rely on network reaction times.

Request Sample PDF Report at: <https://www.alliedmarketresearch.com/request-sample/12853>

The primary driver of the software-defined security market is the growing demand for enhanced network security. With the increase in the number of cyber attacks and data breaches, there has been a rising need for more robust and agile security solutions that can effectively protect networks and data. Software-defined security provides a more flexible and scalable approach to network security, enabling organizations to adapt to changing threat landscapes and respond to security incidents in real-time. This has resulted in an increased adoption of software-defined security solutions by enterprises across various industries.

Another driver of the software-defined security market is the growing adoption of cloud computing and virtualization. The traditional perimeter-based security approach is no longer sufficient to secure networks that are constantly evolving and expanding across multiple locations and cloud environments. Software-defined security solutions provide a more effective

way to secure virtualized environments and cloud-based applications, enabling organizations to maintain a consistent security posture across all their environments. As the adoption of cloud computing and virtualization continues to increase, the demand for software-defined security solutions is expected to grow significantly in the coming years.

Inquire Here Before Buying: <https://www.alliedmarketresearch.com/purchase-enquiry/12853>

One of the significant trends in the software-defined security market is the adoption of artificial intelligence (AI) and machine learning (ML) technologies. AI and ML can analyze vast amounts of data and identify anomalies that may indicate potential security threats, enabling organizations to respond quickly and proactively to security incidents. As a result, there has been an increasing demand for software-defined security solutions that incorporate AI and ML capabilities, such as anomaly detection and behavior analysis.

Another trend in the software-defined security market is the convergence of security and networking. With the rise of software-defined networking (SDN) and network function virtualization (NFV), security is becoming more integrated into the network infrastructure. This approach enables organizations to centralize security policies and management, making it easier to implement and enforce security measures across all network endpoints. As a result, there has been a growing demand for software-defined security solutions that can integrate with SDN and NFV architectures, enabling organizations to achieve a more holistic and efficient approach to network security.

If you have any special requirements, please let us know:

<https://www.alliedmarketresearch.com/request-for-customization/12853>

The global software defined security market has seen a huge uptick as a result of the COVID-19 epidemic, and this trend is expected to continue. This is due to the rapid global spread of the coronavirus, which during the COVID-19 pandemic prompted many organisations to adopt remote working and work from home practises. For many businesses, it can be expensive, time-consuming, and even impractical to deploy expensive network security hardware at these newly developed endpoints (created by remote employees). As a result, many companies have opted to use software defined security market growth for their enterprise security infrastructure and employee data security.

Some of the key companies mentioned within the report are Check Point Software, Technologies Ltd., Cisco Systems, Inc., Intel Corporation, VMware, Inc., Symantec Corporation, EMC Corporation, Fortinet, Inc., Juniper Networks, Inc., and Palo Alto Networks.

Procure Complete Report (343 Pages PDF with Insights, Charts, Tables, and Figures) at:

<https://bit.ly/3nTmSGC>

Access Full Summary of Report: <https://www.alliedmarketresearch.com/software-defined->

Thanks for reading this article; you can also get individual chapter-wise sections or region-wise report versions like North America, Europe, or Asia.

If you have any special requirements, please let us know and we will offer you the report as per your requirements.

Lastly, this report provides market intelligence most comprehensively. The report structure has been kept such that it offers maximum business value. It provides critical insights into the market dynamics and will enable strategic decision-making for the existing market players as well as those willing to enter the market.

David Correa

Allied Analytics LLP

+ +1-800-792-5285

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/633601630>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.