

Endpoint Security Market Grow at Exponential CAGR of 8.4% by 2031 | AO Kaspersky Lab, Broadcom, Microsoft Corporation

Surge in use of bring your own devices (BYOD) and rise in number of connected devices drive the growth of the global endpoint security market.

WILMINGTON, NEW CASTLE, DE, UNITED STATES, December 9, 2024 /EINPresswire.com/ -- The global [endpoint security market](#) was valued at \$14.6 billion in 2021, and is projected to reach \$31.9 billion by 2031, growing at a CAGR of 8.4% from 2022 to 2031. Endpoint security is a

critically important step in securing the endpoint devices such as desktop computers, laptops, mobile devices, and others as this serves as entry to any structured network. Endpoint security technologies come with a number of advantages, including protection for weak services, network security for cloud and internet security, and improved data privacy and policy compliance. Endpoint security has grown significantly in importance over the past few years and has integrated itself into everyday living for people who own smartphones, computers, and other smart devices. Furthermore, organizations are now more vulnerable to risks like organized crime, malicious and unintentional insider threats, hacking activities, and rapid digitization across sectors. As the first line of defense in cybersecurity, endpoint security is extensively used.

For more information, contact Allied Market Research (1000 17th Street, Suite 1000 - 470, New York, NY) at:

<https://www.alliedmarketresearch.com/request-sample/A08314>

Region wise, the [endpoint security market size](#) was dominated by North America in 2021 and is expected to retain its position during the forecast period, owing to the increased number of connected devices in use that has also increased the security risks faced by organizations. However, Asia-Pacific is expected to witness the highest growth in the upcoming years, owing to rapid growth in technologies such as AI, IoT, connected devices, cloud services is attributed to



the high demand of high endpoint device protection in Asia-Pacific. Key players in the Asia-Pacific region are adapting strategies such as acquisition and collaboration to improve endpoint security market analysis.

Depending on end user, the IT and telecom segment dominated the endpoint security market share in 2021 and is expected to continue this dominance during the forecast period, owing to increased usage of mobile devices among mass population. Moreover, security analysts, threat hunters, and IT professionals can assess and stop follow-on threats considerably and more swiftly owing to sophisticated analysis tools and capabilities of endpoint security tools. However, the healthcare segment is expected to witness the highest growth in the upcoming years, owing to enable safer, quicker and more convenient interaction between medical professionals and their medical assistants. Endpoint security is gaining popularity in the healthcare industry due to its increased end-to-end security with regard to patient data, cost advantages, and user-friendly networking features.

Endpoint Security & Threat Intelligence Market Analysis Report :

<https://www.alliedmarketresearch.com/endpoint-security-market/purchase-options>

By deployment mode, the on-premise segment held the major share in 2021, garnering around two-thirds of the global endpoint security market revenue. The cloud segment would also showcase the fastest CAGR of 10.3% during the forecast period, owing to the flexibility and financial advantages that come with cloud services.

By enterprise size, the large enterprise segment held the major share in 2021, garnering more than three-fifths of the global endpoint security market revenue. The small and medium-sized enterprises (SMEs) segment would also showcase the fastest CAGR of 10.1% during the forecast period, owing to a surge in the number of SMEs in Asia-Pacific's region, including China, Japan, and India.

Furthermore, factors such as increased use of bring your own devices (BYOD) and number of connected devices primarily drive the [growth of the endpoint security market](#). However, lack of skilled workers hampers market growth to some extent. Moreover, the increase in adoption of AI enabled automated responses is expected to provide lucrative opportunities for endpoint security market forecast.

Endpoint Security & Threat Intelligence Market Analysis Report :

<https://www.alliedmarketresearch.com/request-for-customization/A08314>

The COVID-19 pandemic has had a negative impact on a number of countries worldwide. Complete lockdown, social isolation, and quarantine, among other pandemic response tactics, have had a negative effect on several global industries, including a portion of the IT security sector. Enterprise virtual private network (VPN) servers were essential to groups and institutions because so many workers now worked from home and so many students were enrolled in online

courses. As a result, businesses faced greater cyber risks and threats as a result of the quick adoption of new ideas. There has been an increasing number of COVID-19 websites offering fake propositions in return for personal information, which is one of the main reasons why attacks on corporate emails have increased. Thus, organizations were anticipated to implement endpoint security solutions during the COVID-19 outbreak by promoting social seclusion at work and permitting remote work-from-home offices. This has helped accelerate the uptake of cloud infrastructure and services, which has increased the market's active device base quickly. This resulted in quick adoption of endpoint security solutions and growth in the market.

More information: <https://www.alliedmarketresearch.com/purchase-enquiry/A08314>

Endpoint Security Market - <https://www.alliedmarketresearch.com/endpoint-security-market-A08314>

The endpoint security market is expected to reach \$31.89 billion by 2031, during the forecast period. The market is driven by the increasing number of cyberattacks and the need for organizations to protect their data and systems. The market is also driven by the increasing adoption of cloud services and the need for organizations to protect their data and systems in the cloud. The market is also driven by the increasing adoption of mobile devices and the need for organizations to protect their data and systems on mobile devices. The market is also driven by the increasing adoption of IoT devices and the need for organizations to protect their data and systems on IoT devices. The market is also driven by the increasing adoption of smart home devices and the need for organizations to protect their data and systems on smart home devices. The market is also driven by the increasing adoption of smart cars and the need for organizations to protect their data and systems on smart cars. The market is also driven by the increasing adoption of smart cities and the need for organizations to protect their data and systems on smart cities. The market is also driven by the increasing adoption of smart infrastructure and the need for organizations to protect their data and systems on smart infrastructure. The market is also driven by the increasing adoption of smart energy and the need for organizations to protect their data and systems on smart energy. The market is also driven by the increasing adoption of smart transportation and the need for organizations to protect their data and systems on smart transportation. The market is also driven by the increasing adoption of smart healthcare and the need for organizations to protect their data and systems on smart healthcare. The market is also driven by the increasing adoption of smart education and the need for organizations to protect their data and systems on smart education. The market is also driven by the increasing adoption of smart entertainment and the need for organizations to protect their data and systems on smart entertainment. The market is also driven by the increasing adoption of smart retail and the need for organizations to protect their data and systems on smart retail. The market is also driven by the increasing adoption of smart manufacturing and the need for organizations to protect their data and systems on smart manufacturing. The market is also driven by the increasing adoption of smart agriculture and the need for organizations to protect their data and systems on smart agriculture. The market is also driven by the increasing adoption of smart defense and the need for organizations to protect their data and systems on smart defense. The market is also driven by the increasing adoption of smart space and the need for organizations to protect their data and systems on smart space. The market is also driven by the increasing adoption of smart infrastructure and the need for organizations to protect their data and systems on smart infrastructure. The market is also driven by the increasing adoption of smart energy and the need for organizations to protect their data and systems on smart energy. The market is also driven by the increasing adoption of smart transportation and the need for organizations to protect their data and systems on smart transportation. The market is also driven by the increasing adoption of smart healthcare and the need for organizations to protect their data and systems on smart healthcare. The market is also driven by the increasing adoption of smart education and the need for organizations to protect their data and systems on smart education. The market is also driven by the increasing adoption of smart entertainment and the need for organizations to protect their data and systems on smart entertainment. The market is also driven by the increasing adoption of smart retail and the need for organizations to protect their data and systems on smart retail. The market is also driven by the increasing adoption of smart manufacturing and the need for organizations to protect their data and systems on smart manufacturing. The market is also driven by the increasing adoption of smart agriculture and the need for organizations to protect their data and systems on smart agriculture. The market is also driven by the increasing adoption of smart defense and the need for organizations to protect their data and systems on smart defense. The market is also driven by the increasing adoption of smart space and the need for organizations to protect their data and systems on smart space.

By solution type, in 2021, the endpoint protection platform segment was the highest revenue contributor to the market, with an 7.3% impressive CAGR. However, the endpoint detection and response segment is estimated to reach \$31.89 billion by 2031, during the forecast period.

By deployment mode, in 2021, the on-premise segment was the highest revenue contributor to the market, with an 7.3% impressive CAGR. However, the cloud segment is estimated to reach \$12.96 billion by 2031, during the forecast period.

By industry vertical, the IT and telecom segment is estimated to reach \$4.91 billion by 2031, with an 4.5% impressive CAGR, during the forecast period. However, healthcare segments are expected to witness approximately 10.2% CAGRs, respectively, during the forecast period respectively.

Region-wise, the endpoint security market growth was dominated by North America. However, Asia-Pacific and Europe are expected to witness a significant growth rate during the forecasted period.

More information: <https://www.alliedmarketresearch.com/endpoint-security-market-A08314>

Emotion AI Market - <https://www.alliedmarketresearch.com/emotion-ai-market-A231628>

Security as a Service Market - <https://www.alliedmarketresearch.com/security-as-a-service-market>

Security as a Service Market - <https://www.alliedmarketresearch.com/security-as-a-service-market>

Cloud Computing Services Market - <https://www.alliedmarketresearch.com/cloud-computing-services-market>

David Correa

Allied Market Research

+1 800-792-5285

[email us here](#)

Visit us on social media:

[Facebook](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/767414196>

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.

© 1995-2024 Newsmatics Inc. All Right Reserved.