# Endpoint Security Market valued over US$9.431 billion in 2021, to experience significant growth

*The endpoint security market was valued at US$9.431 billion in 2021.*

NOIDA, UTTAR PARDESH, INDIA, January 12, 2024 /EINPresswire.com/ -- According to a new report published by Knowledge Sourcing Intelligence, forecasted between 2021 and 2028, the endpoint security market was valued at US$9.431 billion in 2021 and is anticipated to propel significantly over the coming years.

> The endpoint security market was valued at US$9.431 billion in 2021."
> *Knowledge Sourcing Intelligence*

Increased security adoption across many applications such as IT & Telecom, BSFI, and retail is a significant driver fueling the development of the Global Endpoint Security Market. Additionally, the rising number of workplace endpoints and mobile devices with critical data access has generated a massive market for endpoint security solutions. Furthermore, the rising trend of virtualization separates physical systems into several virtual computers, necessitating endpoint security and driving up the need for endpoint security. Moreover, many big and small organizations are embracing the BYOD trend, which is leading to a spike in new and unexpected assaults on the organization's endpoint network, and the high incidence of such attacks is producing a demand for endpoint security, which is driving development in the Global Endpoint Security Market.

Endpoint security includes preventing malicious threats and cyberattacks from exploiting the data and workflow of end-user devices such as laptops, desktops, and mobile phones. It operates by inspecting files that enter the network and safeguarding endpoints via application control and encryption. It offers a consolidated solution that simplifies security administration, enhances business resilience, and boosts total income. Endpoint detection and response (EDR) capabilities are now being offered by market participants to identify sophisticated threats such as polymorphic assaults, fileless malware, and zero-day attacks. The increasing volume and complexity of cybersecurity threats, including hacktivism, organized crime, and purposeful and unintentional insider assaults, can result in the loss of sensitive data, economic insolvency, and

huge reputational costs. As a result, enterprises across industries are using endpoint security solutions to identify, analyze, prohibit, and contain the usage of hazardous or unauthorized programs, therefore preventing data loss. Furthermore, the growing trend of bring your device (BYOD) and remote work policies in small and medium-sized organizations (SMEs) is fueling the demand for enhanced endpoint security solutions to accelerate detection and remediation reaction times.

The market is witnessing multiple collaborations and technological advancements, for instance, WatchGuard Technologies announced Aether 14 and WG Cloud, their newest Endpoint Security Release, in November 2022, with numerous notable functionalities. Endpoint Risk Monitoring stands out as a notable improvement, giving increased monitoring and insight into endpoint security threats and bolstering the overall protection provided by the system.

Access sample report or view details: https://www.knowledge-sourcing.com/report/endpoint-security-market

Based on endpoint type the global endpoint security market is divided into computers & laptops, smartphones, IoT devices, and others. In the worldwide endpoint security industry, IoT devices are predicted to increase significantly in the future years. The expansion of Internet of Things (IoT) devices across industries such as healthcare, manufacturing, and smart homes has expanded the attack surface for cyber-attacks. As more devices become linked, the number of vulnerabilities and possible entry points for malevolent actions grows. As a result, the requirement to protect sensitive data and preserve the integrity of important systems is expected to fuel a spike in demand for comprehensive endpoint security solutions for IoT devices. Considering the continuous development of IoT deployments in both consumer and industrial settings, the IoT endpoint security market is expected to grow significantly, indicating the growing realization of the significance of safeguarding networked devices.

Based on security type the global endpoint security market is divided into endpoint detection and response, endpoint protection platform, mobile threat defence, and others. As a consequence of increased cyber threats and the increasing usage of remote work and mobile devices, the endpoint protection platform (EPP) industry is positioned for considerable development in the coming years. As enterprises' digital footprints grow, the requirement for comprehensive solutions that can protect endpoints in a variety of scenarios becomes critical. Endpoint protection solutions include integrated security capabilities such as antivirus, anti-malware, firewall, and device control, allowing for a comprehensive defence against changing cyber threats. With the continual advancement of complex attack strategies, enterprises are anticipated to prioritize EPP solutions to offer comprehensive endpoint protection, making it a significant driver of the worldwide endpoint security market's substantial expansion.

Based on enterprise size the global endpoint security market is divided into small & medium and large. Among these, the small and medium enterprise size is anticipated to grow significantly over the forecast period. SMEs operate in industries that have strict data privacy and security

regulations, such as healthcare, banking, and law. Endpoint security solutions help SMEs satisfy these compliance criteria by offering features such as data encryption, access limits, and activity monitoring. By assuring compliance, SMEs can avoid legal penalties, financial loss, and reputational harm.

Based on end-user the global endpoint security market is divided into BFSI, government, IT & communications, retail, and others. Among these, the healthcare segment is poised to register high growth over the forecast period. The healthcare sector has seen an increase in cybersecurity risks, such as ransomware attacks, data breaches, and malware infections. Cybercriminals target healthcare businesses because of the rich data they contain and the possible impact on patient safety. These risks have boosted awareness and investment in endpoint security solutions to guard against malicious activity. As a result, the healthcare sector has grown into a key market for endpoint security suppliers.

Based on geography the Asia-Pacific region is anticipated to hold a major market share and is estimated to expand at a high CAGR over the forecast period.  The popularity of BYOD and cloud computing trends is increasing the region's usage of these services. AI, the Internet of Things, the cloud, and other technologies are being quickly adopted by businesses to produce sophisticated security solutions. China is predicted to have a dominant share in the Asia-Pacific market. In China, the rapidly increasing 5G infrastructure is hastening the deployment of endpoint solutions. In addition, due to heightened national security concerns, the Indian government is focusing on data security. Furthermore, the fast growth of businesses in the Asia Pacific area such as banking, healthcare, e-commerce, and manufacturing has resulted in the expansion of IT infrastructure. There is an increasing requirement for comprehensive endpoint security solutions to guard against changing threats as the network of endpoints grows.

As a part of the report, the major players operating in the global endpoint security market, that have been covered are Cisco, Fortinet Inc., Palo Alto Networks, CrowdStrike Holdings Inc., VMware Inc.  Sophos Ltd., Elastic NV, AO Kaspersky Lab.

The market analytics report segments the endpoint security market using the following criteria:

- BY ENDPOINT TYPE

  - Computer & Laptops
  - Smartphones
  - IoT Devices
  - Others

- BY SECURITY TYPE

  - Endpoint Detection and Response
  - Endpoint Protection Platform

- Mobile Threat Defense
- Others

- BY ENTERPRISE SIZE

- Small & Medium
- Large

- BY END-USERS

- BFSI
- Government
- IT & Communications
- Retail
- Others

- BY GEOGRAPHY

- North America

- United States
- Canada
- Mexico

- South America

- Brazil
- Argentina
- Others

- Europe

- Germany
- France
- United Kingdom
- Spain
- Others

- Middle East and Africa

- Saudi Arabia
- UAE
- Others

o  Asia Pacific

- China
- Japan
- South Korea
- India
- Australia
- Others

Companies Profiled:

- Cisco
- Fortinet Inc.
- Palo Alto Networks
- CrowdStrike Holdings Inc.
- VMware Inc.
- Sophos Ltd.
- Elastic NV
- AO Kaspersky Lab

Explore More Reports:

- Security Screening Market: https://www.knowledge-sourcing.com/report/security-screening-market
- Network Security Market: https://www.knowledge-sourcing.com/report/network-security-market
- Email Security Market: https://www.knowledge-sourcing.com/report/email-security-market

Ankit Mishra
Knowledge Sourcing Intelligence LLP
+1 850-250-1698
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn

---

in today's world. Please see our Editorial Guidelines for more information.