+44 20 8123 2220
info@marketpublishers.com

Endpoint Security Market – Global Industry Size, Share, Trends, Opportunity, and Forecast By Solution (Endpoint Protection Platform, Endpoint Detection and Response), By Deployment Mode (On-Premise, Cloud), By Organization Size (Large Enterprises, SMEs), By End User (IT & Telecom, BFSI, Industrial, Education, Retail, Healthcare, Manufacturing, Others), By Region, Competition, 2018-2028

https://marketpublishers.com/r/E19748C1326FEN.html
Date: November 2023
Pages: 188
Price: US$ 4,900.00 (Single User License)
ID: E19748C1326FEN

Abstracts

The projected market size for the global endpoint security market is expected to reach USD 15.73 billion by the end of 2022, with a compound annual growth rate (CAGR) of 9.86% during the forecast period. The global endpoint security market plays a pivotal role in the ever-evolving landscape of cybersecurity. This market focuses on safeguarding various endpoints like computers, smartphones, and servers from a myriad of cyber threats such as malware, ransomware, and phishing attacks. With the rise of remote work, bring-your-own-device (BYOD) practices, and the proliferation of Internet of Things (IoT) devices, the attack surface has expanded significantly. As a result, endpoint security solutions have become essential for organizations to ensure the protection of their sensitive data and digital assets. These solutions encompass a range of technologies including antivirus software, firewalls, intrusion detection systems, and encryption tools, all designed to prevent, detect, and respond to cyber threats. The global endpoint security market continues to evolve in response to the ever-changing threat landscape, with innovations such as AI and machine learning being integrated into solutions to provide proactive threat detection and advanced security capabilities.

Key Market Drivers

+44 20 8123 2220
info@marketpublishers.com

Increasing Network Complexity

The escalating complexity of networks is emerging as a significant driver behind the growth of the global endpoint security market. As organizations expand their digital footprint, incorporating cloud services, remote work environments, and a diverse range of Internet of Things (IoT) devices, the network architecture becomes increasingly intricate. This complexity creates numerous entry points for cyber threats, making endpoint security a crucial defense mechanism. With a multitude of devices and endpoints accessing critical data and applications, the potential attack surface expands, requiring comprehensive solutions that can safeguard each endpoint effectively.

The intricate network environment demands advanced endpoint security solutions that can adapt to evolving threats and offer real-time protection. Traditional security measures can struggle to cope with the multifaceted nature of modern networks, leading to gaps in defense that cybercriminals can exploit. Endpoint security technologies, equipped with artificial intelligence, machine learning, and behavior-based analytics, provide the agility required to counteract dynamic threats across the intricate network landscape. As organizations continue to embrace digital transformation and adopt emerging technologies, the demand for robust endpoint security solutions will only intensify. The increasing network complexity underscores the importance of securing endpoints at every level to ensure the overall integrity, confidentiality, and availability of sensitive data and digital assets.

The Increase in Remote Work and Mobile Device Usage

The surge in remote work and the widespread use of mobile devices are serving as significant catalysts driving the growth of the global endpoint security market. With the advent of flexible work arrangements and the proliferation of mobile devices, employees are accessing sensitive corporate data and applications from various locations and devices, extending the traditional network perimeter. This expanded remote and mobile workforce creates new entry points for cyber threats, making endpoint security a critical necessity. Endpoint security solutions have become essential tools for safeguarding the diverse range of devices that connect to organizational networks, including laptops, smartphones, tablets, and IoT devices. The decentralization of work environments necessitates security measures that can effectively protect data, prevent unauthorized access, and mitigate the risk of breaches and data leaks.

To address these challenges, organizations are adopting advanced endpoint security

solutions equipped with capabilities like real-time threat detection, behavior-based analysis, and secure access controls. These technologies ensure that regardless of the device or location, sensitive information remains protected from cyber threats. As remote work and mobile device usage continue to shape the modern work landscape, the demand for robust and adaptable endpoint security solutions is poised to rise. Organizations recognize that a comprehensive approach to endpoint security is pivotal in maintaining data integrity, complying with regulations, and safeguarding their reputation in an increasingly digital and interconnected world.

The Adoption of Bring-Your-Own-Device (BYOD) Policies

The adoption of Bring-Your-Own-Device (BYOD) policies is exerting a notable influence on the global endpoint security market. As organizations increasingly embrace the concept of employees using personal devices for work-related tasks, the boundaries between personal and professional environments become blurred. This trend introduces unique security challenges, as diverse devices access sensitive corporate data and networks. To mitigate the risks associated with BYOD, organizations are turning to robust endpoint security solutions that offer comprehensive protection across various devices and operating systems. These solutions encompass advanced features such as device management, data encryption, secure access controls, and real-time threat detection. The implementation of effective endpoint security measures not only ensures the protection of sensitive data but also enables organizations to strike a balance between enabling flexible work practices and maintaining the highest standards of security in the face of evolving cyber threats.

The Adoption of Emerging Technologies

The rapid adoption of emerging technologies is a driving force behind the global endpoint security market. As organizations integrate innovative technologies like cloud computing, Internet of Things (IoT) devices, and artificial intelligence (AI), the attack surface expands, creating new avenues for cyber threats. To counter these evolving risks, endpoint security solutions are evolving to incorporate these very technologies. AI and machine learning enable proactive threat detection by analyzing patterns and anomalies, while cloud-based solutions offer scalability and centralized management for diverse endpoints. Moreover, as IoT devices become integral to business operations, securing these endpoints becomes critical. The integration of advanced technologies into endpoint security not only enhances protection but also empowers organizations to adapt to dynamic threat landscapes and ensure the resilience of their digital infrastructure in the face of ever-evolving cyber threats.

+44 20 8123 2220
info@marketpublishers.com

Key Market Challenges

Increasing Complexity and Diversity of Cyber Threats

The global endpoint security market is grappling with the challenge posed by the increasing complexity and diversity of cyber threats. As cybercriminal tactics become more sophisticated and diverse, the landscape of potential threats continues to expand, making it harder for traditional endpoint security solutions to keep up. The emergence of new malware variants, advanced persistent threats (APTs), zero-day vulnerabilities, and polymorphic malware creates a multifaceted threat landscape that requires agile and adaptive defense mechanisms. This complexity can overwhelm organizations and result in gaps in security coverage, leaving endpoints vulnerable to attacks. As a response, the endpoint security market is evolving to integrate advanced technologies like artificial intelligence (AI) and machine learning (ML) to detect and respond to emerging threats in real-time. Additionally, cybersecurity professionals are increasingly embracing threat intelligence and collaborative approaches to stay ahead of the evolving tactics of cyber adversaries and bolster the resilience of endpoint security measures.

The Shortage of Skilled Cybersecurity Professionals

The shortage of skilled cybersecurity professionals is proving to be a significant hindrance to the growth of the global endpoint security market. As the demand for robust endpoint security solutions increases, the shortage of qualified experts capable of implementing, managing, and optimizing these solutions becomes more pronounced. The intricacies of modern cyber threats and the evolving technology landscape require specialized knowledge and skills to effectively configure and operate endpoint security tools. The lack of skilled professionals not only impacts an organization's ability to implement effective security measures but also contributes to delays in incident response and threat detection. To address this challenge, organizations are investing in training programs, partnering with managed security service providers (MSSPs), and seeking ways to attract and retain cybersecurity talent. Bridging the skills gap is imperative to ensure that endpoint security measures remain effective and responsive in the face of an ever-changing threat landscape.

Key Market Trends

The Growing Emphasis on User Privacy

+44 20 8123 2220
info@marketpublishers.com

The growing emphasis on user privacy is exerting a significant impact on the global endpoint security market. With increasing awareness of data breaches and privacy concerns, individuals and regulatory bodies are demanding stronger protection of personal information. As organizations collect and process vast amounts of sensitive data, the need to safeguard this data from unauthorized access and potential breaches has become paramount. Endpoint security solutions are evolving to include robust privacy features such as data encryption, secure authentication methods, and access controls that ensure only authorized users can access sensitive information. This heightened focus on user privacy not only aligns with ethical considerations but also with regulatory requirements like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). By integrating enhanced privacy measures into endpoint security, organizations demonstrate their commitment to respecting user privacy rights while fortifying their defenses against potential security breaches and maintaining trust with their customers and stakeholders.

The shift towards Zero-Trust Security Architectures

The global endpoint security market is experiencing the significant influence of the shift towards Zero-Trust security architectures. Traditional perimeter-based security models are no longer sufficient in today's complex threat landscape, where breaches can occur both from external and internal sources. Zero-Trust architecture advocates for a paradigm shift that assumes no inherent trust, requiring strict verification for all users and devices attempting to access a network or resources. This approach aligns with the evolving nature of cyber threats and the increasing sophistication of attacks. Endpoint security solutions are adapting to this trend by incorporating Zero-Trust principles, including identity verification, continuous monitoring, and least privilege access controls. By enforcing security measures at the endpoint level, organizations can significantly mitigate risks, prevent lateral movement within networks, and ensure that only authorized entities gain access, contributing to a more resilient and adaptable security posture.

Segmental Insights

Deployment Mode Insights

Based on deployment mode, the cloud segment emerges as the predominant segment, exhibiting unwavering dominance projected throughout the forecast period. As organizations seek flexible and scalable security solutions, the cloud-based approach offers streamlined implementation, central management, and reduced infrastructure

+44 20 8123 2220
info@marketpublishers.com

complexities. This deployment mode aligns with the increasing adoption of cloud services and remote work environments, allowing seamless protection of distributed endpoints. The cloud segment's prevalence underscores its efficacy in addressing modern cybersecurity challenges, positioning it as a go-to choose for organizations aiming to enhance their endpoint security measures efficiently and adapt to evolving threat landscapes.

End User Insights

Based on end user, the manufacturing segment emerges as a formidable frontrunner, exerting its dominance and shaping the market's trajectory throughout the forecast period. Manufacturing industries increasingly rely on interconnected systems, industrial IoT devices, and automation, creating a heightened need for robust endpoint security solutions. With critical operational processes and sensitive intellectual property at stake, manufacturing companies are prioritizing comprehensive protection for their endpoints. The sector's leadership in adopting advanced security measures not only safeguards production processes but also bolsters the overall resilience of the industry against cyber threats. As manufacturing continues to drive innovation, its proactive stance towards endpoint security solidifies its role in shaping the market's direction for the foreseeable future.

Regional Insights

North America stands poised to uphold its dominant stance in the global endpoint security market, underscoring its pivotal role in molding the industry's landscape. The region's technological advancement, robust cybersecurity ecosystem, and significant investments in cutting-edge security solutions contribute to its continued leadership. With a thriving business landscape, increasing digitalization, and a high concentration of industries vulnerable to cyber threats, North American organizations prioritize robust endpoint security to safeguard their critical assets. Additionally, the region's stringent regulatory landscape and the growing awareness of cybersecurity risks further drive the demand for advanced endpoint security measures. North America's leadership not only underscores its commitment to ensuring the highest level of security but also solidifies its influence in driving innovation and best practices within the global endpoint security market.

Key Market Players

VMware Inc.

+44 20 8123 2220
info@marketpublishers.com

Bitdefender LLC

Avast Software SRO

Fortinet Inc.

ESET LLC

Panda Security SL

Kaspersky Lab Inc.

Microsoft Corporation

Sophos Group PLC

Cisco Systems Inc.

Report Scope:

In this report, the global endpoint security market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Global Endpoint Security Market, By Solution:

Endpoint Protection Platform

Endpoint Detection and Response

Global Endpoint Security Market, By Deployment Mode:

On-premises

Cloud

Global Endpoint Security Market, By Organization Size:

+44 20 8123 2220
info@marketpublishers.com

SMEs

Large Enterprises

Global Endpoint Security Market, By End User:

IT & Telecom

BFSI

Industrial

Education

Retail

Healthcare

Manufacturing

Others

Global Endpoint Security Market, By Region:

North America

Europe

South America

Middle East & Africa

Asia Pacific

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Endpoint Security Market.

+44 20 8123 2220
info@marketpublishers.com

Available Customizations:

Global Endpoint Security market report with the given market data, Tech Sci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

9. EUROPE ENDPOINT SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

10. SOUTH AMERICA ENDPOINT SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

11. MIDDLE EAST & AFRICA ENDPOINT SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

12. ASIA PACIFIC ENDPOINT SECURITY MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

15. COMPANY PROFILES

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Endpoint Security Market – Global Industry Size, Share, Trends, Opportunity, and Forecast By Solution (Endpoint Protection Platform, Endpoint Detection and Response), By Deployment Mode (On-Premise, Cloud), By Organization Size (Large Enterprises, SMEs), By End User (IT & Telecom, BFSI, Industrial, Education, Retail, Healthcare, Manufacturing, Others), By Region, Competition, 2018-2028

Product link: https://marketpublishers.com/r/E19748C1326FEN.html

Price: US$ 4,900.00 (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/E19748C1326FEN.html

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:
Last name:
Email:
Company:
Address:
City:
Zip code:
Country:
Tel:
Fax:
Your message:

**All fields are required

Custumer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at https://marketpublishers.com/docs/terms.html

+44 20 8123 2220
info@marketpublishers.com

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970