Advanced Persistent Threat Market Size Worth $30.9 Billion by 2030 | CAGR 20.5%

WILMINGTON, NEW CASTLE, DE, UNITED STATES, September 19, 2025 /EINPresswire.com/ -- According to a new report published by Allied Market Research, titled, “Advanced Persistent Threat Market," The advanced persistent threat market was valued at $5.9 billion in 2021, and is estimated to reach $30.9 billion by 2030, growing at a CAGR of 20.5% from 2022 to 2030.

An Advanced Persistent Threat (APT) is a network attack in which cybercriminals enter a computer or network and use it (its system) to conduct undetected operations. APT attacks are mostly directed at companies that handle highly secret data, such as governmental and financial institutions.

Since APT do not appear to be malware at first glance and can infiltrate themselves quite deeply in an administration's IT systems, and are particularly difficult to identify and remove. The APT's developers and designers are continuously keeping an eye on it and directing its actions by updating their code to evade detection and morph it into a changing set of characteristics. Moreover, a penetrated company won't even be aware of it; they might not learn about it until much later through log analysis monitoring with Security Information and Event Management (SIEM) solutions or by outbound communication activities.

□□□□□□□□ □□□□□□□ □□□□□□□ (□□□ □□□□ □□□□□□□□□ □□ □□□ – 230 □□□□□□) □□: https://www.alliedmarketresearch.com/request-sample/A31423

Cyber threats are not only affecting the productivity of businesses but also harming essential IT infrastructure and sensitive data of firms. There is a surge in the frequency of cybercrimes because of the quick growth of digital transactions across all industrial verticals. The market for cyber security goods and services is being driven by the rise in enterprise data breaches or data leaks. This increase is attributable to technologies such as Machine Learning (ML), which enable

attackers to produce several variants of harmful code every day. Malware bytes also notes that state-sponsored APT organizations and online criminals have switched to using COVID-19 lures. Attacks include lure documents with links to malicious Microsoft Office templates, malicious macros, RTF exploits using OLEI-related vulnerabilities, and malicious LNK files.

Advanced persistent threats are diverse in nature, long-lasting, and highly targeted. Due to the emergence of several new zero day threats, the security needs are also changing as a result of changes in the business environment. Businesses are at danger due to this lack of knowledge about advanced security risks, which is also slowing the demand for advanced persistent threat prevention. Enterprises generally lack a lot of understanding regarding APTs and effective defense strategies.

Concerns about security have increased dramatically as a result of the rising trend of a gazillion gigabytes of sensitive data flowing to the cloud, since cyber attackers are now a serious threat. Companies that rely too much on cloud-based business models are now more vulnerable than ever to a variety of cyber threats. The goal of security is the continuous and continuing assessment of risks and uncertainties. Data breaches have become a very common occurrence due to the massive volume of data produced by IoT devices, data loss prevention technologies, and security information (security solutions) in industry 4.0. In order to deal with these data breaches, firms are choosing advanced analytics, strict access controls, and technology.

The global advanced persistent threat market share is segmented based on deployment mode, services, solutions, and region. By deployment mode, it is classified into cloud and on-premise. By services, it is classified into Security Information and Event Management (SIEM), endpoint protection, Intrusion Detection System/ Intrusion Prevention System (IDS/ IPS), sandboxing, Next-Generation Firewall (NGFW), forensic analysis and other. By region, the market is analyzed across North America, Europe, Asia-Pacific, and LAMEA.

The key players profiled in the advanced persistent threat industry report include Cisco Systems, Inc., AO Kaspersky Lab., ESET spol. S r.o., Sophos Ltd., Forcepoint, VMware, Inc, Microsoft, Palo Alto Networks, McAfee, LLC, and F-Secure.

The report offers a comprehensive analysis of the global advanced persistent threat protection market trends by thoroughly studying different aspects of the market including major segments, market statistics, market dynamics, regional market outlook, investment opportunities, and top players working towards growth of the market. The report also sheds light on the present scenario and upcoming trends & developments that are contributing to the growth of the market. Moreover, restraints and challenges that hold power to obstruct the market growth are also profiled in the report along with the Porter’s five forces analysis of the market to elucidate factors such as competitive landscape, bargaining power of buyers and suppliers, threats of new players, and emergence of substitutes in the market.

The study provides a detailed global advanced persistent threat market analysis, advanced

persistent threat market size, and global advanced persistent threat market forecast from 2022 - 2030.

Impact of COVID-19 on the Global Advanced Persistent Threat Protection Industry

Due to the COVID-19 pandemic outbreak, the world's economies are currently experiencing a severe crisis

Coronavirus-based hacking has been used by a number of Advanced Persistent Threat (APT) groups, including those funded by governments and cybercriminals, to infect victims' computers and spread malware

For instance, the North Korean-based threat group Kimsuky started employing spear-phishing emails with the topic COVID-19 in March 2020, as its first infection vector

The emails have malicious attachments and a bug that enables remote code execution by taking advantage of a weakness in the Microsoft Office OLE interface to spread malware

□□□ □□□ & □□□ □□□□□□□□□ □□□□□□□□ □□ □□□□ □□□□□□ (230 □□□□□ □□□ □□□□ □□□□□□□□, □□□□□□, □□□□□□, □□□ □□□□□□□) □□: https://www.alliedmarketresearch.com/advanced-persistent-threat-market/purchase-options

Key Findings of the Study

Based on deployment mode, the on-premise sub-segment emerged as the global leader in 2021 and the cloud sub-segment is anticipated to be the fastest growing sub-segment during the forecast period

Based on services, the managed services sub-segment emerged as the global leader in 2021 and the professional services sub-segment is anticipated to be the fastest growing sub-segment during the forecast period

Based on solutions, the Security Information and Event Management (SIEM) sub-segment emerged as the global leader in 2021 and the Next-generation Firewall (NGFW) sub-segment is predicted to show the fastest growth in the upcoming years

Based on region, the North America market registered the highest market share in 2021 and Asia-Pacific is projected to show the fastest growth during the forecast period

Browse More Trending Reports :

Synthetic Data Generation Market
https://www.alliedmarketresearch.com/voice-cloning-market

Virtual Customer Premises Equipment Market https://www.alliedmarketresearch.com/virtual-customer-premises-equipment-market-A127111

RAN Intelligent Controller Market
https://www.alliedmarketresearch.com/ran-intelligent-controller-market-A156655

Email Encryption Software Market
https://www.alliedmarketresearch.com/email-encryption-software-market-A132488

Intellectual Property Management Market
https://www.alliedmarketresearch.com/intellectual-property-management-market-A108500

Mobile 3D Market
https://www.alliedmarketresearch.com/mobile-3d-market

About Us :

Allied Market Research (AMR) is a full-service market research and business-consulting wing of Allied Analytics LLP based in Wilmington, Delaware. Allied Market Research provides global enterprises as well as medium and small businesses with unmatched quality of "Market Research Reports" and "Business Intelligence Solutions." AMR has a targeted view to provide business insights and consulting to assist its clients to make strategic business decisions and achieve sustainable growth in their respective market domain.

We are in professional corporate relations with various companies, and this helps us in digging out market data that helps us generate accurate research data tables and confirms utmost accuracy in our market forecasting. Each and every data presented in the reports published by us is extracted through primary interviews with top officials from leading companies of domain concerned. Our secondary data procurement methodology includes deep online and offline research and discussion with knowledgeable professionals and analysts in the industry.

David Correa
Allied Market Research
+ +1 800-792-5285
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X