+357 96 030922
info@marketpublishers.com

Threat Hunting Market Forecasts to 2030 – Global Analysis By Offering (Tool and Service), Threat Type (Advanced Persistent Threats (APTs), Malware and Ransomware, Insider Threats, Phishing and Social Engineering, DDoS, Zero-Day Exploits and Other Threat Types), Enterprise Size, Deployment Mode, End User and By Geography

https://marketpublishers.com/r/T50AB81DB922EN.html
Date: February 2025
Pages: 150
Price: US$ 4,150.00 (Single User License)
ID: T50AB81DB922EN

Abstracts

According to Stratistics MRC, the Global Threat Hunting Market is accounted for $3.52 billion in 2024 and is expected to reach $8.98 billion by 2030 growing at a CAGR of 16.9% during the forecast period. Threat hunting is a proactive approach to cybersecurity that aims to find and eliminate possible threats before they have a chance to do serious harm. Threat hunting is the process of actively looking for indications of malicious activity within a network or system, as opposed to traditional security measures that rely. Professionals in cybersecurity, also known as threat hunters, use a variety of instruments, methods, and data analytics to find irregularities, weaknesses, or indicators of compromise (IOCs). Threat hunting helps organizations stay ahead of cybercriminals and enhances the overall security posture by continuously examining patterns and behaviours.

According to a 2019 survey by the SANS Institute, 61% of respondents reported at least an 11% measurable improvement in their overall security posture after implementing threat hunting practices.

Market Dynamics:

Driver:

+357 96 030922
info@marketpublishers.com

Growing cyber attacks and data breach incidents

Data breaches have grown to be a major worry for businesses in all industries. Concern over the necessity of strong cybersecurity systems has increased as a result of high-profile events like the Target, Equifax, and Colonial Pipeline hacks. Businesses are spending more money on threat-hunting capabilities since these breaches frequently lead to large financial losses, legal issues, and eroded trust. Additionally, lessening the overall impact and preventing hackers from gaining continuous access to sensitive systems and data, these solutions assist organizations in detecting breaches earlier.

Restraint:

Expensive implementation price

The high expense of implementing threat-hunting solutions is one of the main obstacles that organizations must overcome. Investing in specialized software tools, security infrastructure, and qualified staff is necessary to implement a successful threat-hunting program. Furthermore, there may be significant recurring operational expenses for things like threat-hunting, data analysis, and system maintenance. This expense might be unaffordable for small and medium-sized businesses (SMEs), which would restrict their capacity to adopt such cutting-edge cybersecurity measures.

Opportunity:

Developments in automated threat hunting

Automation in threat hunting is becoming increasingly important as cyber threats continue to grow in complexity. Organizations can scale their threat-hunting activities with automation while preserving accuracy and efficiency. Security staff is less burdened by automated systems' ability to continuously monitor network traffic, analyze massive datasets, and spot possible threats in real time. Additionally, automation can give early warnings of possible security breaches by assisting organizations in identifying threats that conventional methods might miss. Organizations have a great chance to take advantage of automated threat-hunting systems that improve their capacity to stop and address security incidents as automation technologies advance.

Threat:

+357 96 030922
info@marketpublishers.com

Lack of qualified cybersecurity experts

A major obstacle to the market's expansion is the worldwide lack of qualified cybersecurity specialists, even in spite of the rising demand for threat-hunting solutions. Threat hunting is an extremely specialized field that necessitates a thorough comprehension of malware analysis, network behavior, and sophisticated threat detection techniques. However, there is a severe shortage of qualified personnel in the cybersecurity field who can efficiently manage these intricate programs. In furtherance of impeding the expansion of internal threat-hunting initiatives, this shortage makes businesses more dependent on managed services, which might not be a viable or long-term solution for all companies.

Covid-19 Impact:

The COVID-19 pandemic significantly impacted the threat hunting market by speeding up the transition to remote work and digital transformation, both of which raised the risk of cyber attacks. The attack surface grew as businesses quickly embraced remote access and cloud-based services to maintain business continuity, making threat detection and mitigation more difficult. The need for strong threat-hunting tactics was further underscored by the rise in cybercriminal activity, which included ransom ware attacks, phishing campaigns, and data breaches. Moreover, the pandemic highlighted the lack of qualified experts and the increasing difficulty of protecting decentralized networks, even as it spurred increased investment in cybersecurity practices and tools, such as threat-hunting tools.

The Malware and Ransomware segment is expected to be the largest during the forecast period

The malware and ransomware segment is expected to account for the largest market share during the forecast period. With the growing sophistication of ransomware attacks, which have damaged operations and demanded large ransoms from organizations worldwide, these kinds of cyber threats have been on the rise. Since malware can spread quickly and cause serious harm, including data theft, system corruption, and unauthorized access, it remains a serious concern. Additionally, malware can take many different forms, including viruses, trojans, and spyware.

The Healthcare segment is expected to have the highest CAGR during the forecast period

+357 96 030922
info@marketpublishers.com

Over the forecast period, the healthcare segment is predicted to witness the highest growth rate. Healthcare organizations are more vulnerable to cyber attacks as they use digital technologies like telemedicine, electronic health records (EHR), and Internet of Things (IoT) devices. These attacks are especially likely to target sensitive patient data and vital healthcare infrastructure. Cybersecurity has become a top priority due to the increase in ransom ware attacks, data breaches, and the exploitation of healthcare systems. Furthermore, strong threat-hunting solutions are in greater demand as a result of the industry's quick digital transformation and strict legal requirements like HIPAA.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share. The region's power is fuelled by the existence of significant technology firms, sophisticated cybersecurity infrastructure, and a high concentration of big businesses that are progressively implementing threat-hunting solutions to defend vital systems and sensitive data against changing cyber threats. Increased investments in cybersecurity have been prompted by the notable increase in cyber attacks, including ransom ware, data breaches, and advanced persistent threats (APTs), in the United States in particular. Moreover, organizations are also being forced to give proactive threat-hunting tactics top priority by strict regulatory frameworks like the CCPA and GDPR.

Region with highest CAGR:

Over the forecast period, the Asia Pacific (APAC) region is anticipated to exhibit the highest CAGR. The region's attack surface for cyber threats has been greatly expanded by the rapid digital transformation of nations like China, India, Japan, and Southeast Asia, as well as the growing adoption of cloud, IoT, and mobile platforms. Additionally, the rise in cybercrime activities, such as ransom ware attacks, phishing, and data breaches, has led to organizations investing heavily in threat-hunting solutions, and governments in the region are stepping up efforts to improve cybersecurity capabilities through stricter laws and frameworks, which is propelling market growth.

Key players in the market

Some of the key players in Threat Hunting market include Broadcom, Inc., IBM Corporation, Palo Alto Networks, Inc., Check Point Software Technologies Ltd., Symantec, Rapid 7, Verizon Inc, Mindpoint Group, Capgemini, SentinelOne, Inc., Talatek, Sumo Logic, Inc., Cisco Systems, Inc., VMware Inc and CrowdStrike, Inc.

+357 96 030922
info@marketpublishers.com

Key Developments:

In November 2024, Broadcom Inc. and Telia Company announced the expansion of their longtime partnership with a new multi-year agreement, which will see Telia further modernize and transform its telco and cloud infrastructure with the VMware product portfolio.

In July 2024, IBM announced that it has secured a five-year contract with $26 million in initial funding from the U.S. Agency for International Development (USAID) to support its Cybersecurity Protection and Response (CPR) program aimed to expand and enhance the agency's cybersecurity response support for host governments in the Europe and Eurasia (E&E) region.

In May 2024, Palo Alto Networks and IBM unveiled a broad-reaching strategic partnership to strengthen each company's cybersecurity footprint in a move that promises to reshape the cybersecurity landscape. The wide-ranging agreement sees Palo Alto Networks acquiring IBM's QRadar SaaS business and incorporating IBM’s watsonx LLMs into its Cortex XSIAM solution.

Offerings Covered:

- Tool
- Service

Threat Types Covered:

- Advanced Persistent Threats (APTs)
- Malware and Ransomware
- Insider Threats
- Phishing and Social Engineering
- DDoS

+357 96 030922
info@marketpublishers.com

Zero-Day Exploits

Other Threat Types

Enterprise Sizes Covered:

Small and Mid-Sized Enterprises (SMEs)

Large Enterprises

Deployment Modes Covered:

Cloud

On-Premises

End Users Covered:

Banking, Financial Services, and Insurance (BFSI)

IT and ITeS

Government

Energy and Utilities

Manufacturing

Healthcare

Retail & Ecommerce

Others End Users

Regions Covered:

+357 96 030922
info@marketpublishers.com

North America

US

Canada

Mexico

Europe

Germany

UK

Italy

France

Spain

Rest of Europe

Asia Pacific

Japan

China

India

Australia

New Zealand

South Korea

Rest of Asia Pacific

South America

+357 96 030922
info@marketpublishers.com

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

What our report offers:
- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2022, 2023, 2024, 2026, and 2030
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

+357 96 030922
info@marketpublishers.com

- Company Profiling
  - Comprehensive profiling of additional market players (up to 3)
  - SWOT Analysis of key players (up to 3)
- Regional Segmentation
  - Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)
- Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

11 KEY DEVELOPMENTS

12 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Threat Hunting Market Forecasts to 2030 – Global Analysis By Offering (Tool and Service), Threat Type (Advanced Persistent Threats (APTs), Malware and Ransomware, Insider Threats, Phishing and Social Engineering, DDoS, Zero-Day Exploits and Other Threat Types), Enterprise Size, Deployment Mode, End User and By Geography

Product link: https://marketpublishers.com/r/T50AB81DB922EN.html

Price: US$ 4,150.00 (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/T50AB81DB922EN.html