+44 20 8123 2220
info@marketpublishers.com

Threat Hunting Market - Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solutions, Services), By Deployment Mode (On-Premises, Cloud-Based, Hybrid), By Organization Size (Large Enterprises, SMEs), By Industry Vertical (BFSI, Healthcare, Government, Retail, Manufacturing, Telecommunications, Others), By Threat Type (Advanced Persistent Threats, Insider Threats, Malware, Phishing), By Region and Competition, 2019-2029F

https://marketpublishers.com/r/T057213F56D3EN.html
Date: August 2024
Pages: 185
Price: US$ 4,900.00 (Single User License)
ID: T057213F56D3EN

Abstracts

The Global Threat Hunting Market was valued at USD 3.53 Billion in 2023 and is expected to reach USD 10.19 Billion by 2029 with a CAGR of 19.14% during the forecast period.

The global threat hunting market is experiencing robust growth driven by the escalating frequency and sophistication of cyber threats. As organizations increasingly face complex and targeted cyberattacks, the demand for proactive threat detection and response strategies has surged, leading to a significant expansion of the threat hunting market. Threat hunting involves actively searching for signs of malicious activities within an organization’s network, rather than waiting for automated systems to detect and respond to security breaches. This proactive approach helps organizations identify and mitigate threats before they cause significant damage, enhancing overall cybersecurity posture.

+44 20 8123 2220
info@marketpublishers.com

Key drivers of market growth include the rising incidence of advanced persistent threats (APTs), insider threats, and ransomware attacks. Traditional security measures such as firewalls and antivirus software are often inadequate against these sophisticated threats, making threat hunting an essential component of a comprehensive cybersecurity strategy. The increasing adoption of digital technologies, cloud computing, and IoT devices further amplifies the attack surface, necessitating advanced threat hunting solutions to safeguard critical assets and sensitive data.

The market is characterized by a diverse range of solutions and services. Threat hunting platforms, which provide advanced analytics and automated capabilities, are gaining prominence due to their ability to detect anomalies and respond swiftly to potential threats. Managed threat hunting services are also becoming increasingly popular, offering organizations the expertise and resources needed to address complex security challenges without maintaining an in-house team. These services are particularly beneficial for small and medium-sized enterprises (SMEs) that may lack the resources to deploy and manage sophisticated threat hunting tools independently.

Key Market Drivers

Increasing Frequency and Sophistication of Cyber Attacks

The global threat hunting market is significantly driven by the escalating frequency and sophistication of cyber attacks. Traditional security measures, such as firewalls and antivirus software, often struggle to detect and mitigate advanced persistent threats (APTs), zero-day exploits, and ransomware. As attackers employ more sophisticated techniques, including encryption, polymorphic malware, and social engineering, organizations face greater challenges in defending their digital environments. Threat hunting provides a proactive approach to cybersecurity by actively searching for signs of malicious activity within networks and systems, rather than relying solely on automated defenses. This proactive stance allows organizations to identify and address vulnerabilities before they are exploited, reducing the potential impact of breaches. The increasing number of high-profile data breaches and cyber incidents has heightened awareness of the need for advanced threat detection capabilities, driving demand for threat hunting solutions and services. As cyber threats continue to evolve, the market for threat hunting is expected to grow, with organizations investing in advanced tools and expertise to enhance their security posture and safeguard critical assets.

Growing Adoption of Digital Transformation and Cloud Computing

+44 20 8123 2220
info@marketpublishers.com

The rapid adoption of digital transformation and cloud computing is a key driver for the global threat hunting market. As organizations migrate their data and applications to cloud environments and embrace digital technologies, they expand their attack surfaces, creating new opportunities for cyber threats. Cloud computing introduces complexities such as shared responsibility models, multi-cloud environments, and increased data mobility, which can complicate traditional security approaches. Threat hunting tools and services are essential for addressing these challenges, as they offer enhanced visibility and control over cloud-based assets and activities. By leveraging threat hunting solutions, organizations can monitor and analyze data flows, detect anomalies, and respond to potential threats in real time. The integration of threat hunting with cloud security strategies helps organizations protect sensitive information, ensure compliance, and maintain robust defenses against evolving cyber threats. As digital transformation continues to accelerate, the demand for threat hunting solutions that can address the unique security challenges of cloud environments will drive market growth.

Regulatory Compliance and Data Protection Requirements

Regulatory compliance and data protection requirements are significant drivers of the global threat hunting market. Organizations across various industries are subject to stringent regulations designed to protect sensitive data and ensure cybersecurity. Regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) mandate robust security measures and regular monitoring to safeguard personal and financial information. Failure to comply with these regulations can result in severe penalties, legal consequences, and reputational damage. Threat hunting plays a crucial role in helping organizations meet compliance requirements by providing enhanced visibility into network activity, identifying potential security gaps, and ensuring timely response to threats. By integrating threat hunting into their security frameworks, organizations can proactively detect and mitigate risks, maintain compliance with regulatory standards, and avoid costly breaches and fines. The increasing emphasis on data protection and regulatory adherence is expected to drive demand for threat hunting solutions and services.

Advancements in Threat Detection Technologies

Advancements in threat detection technologies are a major driver for the global threat hunting market. The development of sophisticated technologies such as artificial intelligence (AI), machine learning (ML), and behavioral analytics has revolutionized the

+44 20 8123 2220
info@marketpublishers.com

field of threat hunting. These technologies enable more accurate and efficient detection of anomalies, patterns, and indicators of compromise within large volumes of data. AI and ML algorithms can analyze vast datasets, identify emerging threats, and adapt to new attack techniques in real time, enhancing the effectiveness of threat hunting efforts. Additionally, advancements in data analytics, automation, and orchestration have streamlined threat hunting processes, allowing security teams to focus on higher-priority tasks and respond more rapidly to incidents. The continuous evolution of threat detection technologies drives innovation in the threat hunting market, as organizations seek to leverage cutting-edge solutions to stay ahead of cyber adversaries. As technology continues to advance, the demand for advanced threat hunting tools and services will likely grow, further fueling market expansion.

Key Market Challenges

Skill Shortage

The global threat hunting market faces a significant challenge due to the acute shortage of skilled cybersecurity professionals. Threat hunting requires specialized expertise in cybersecurity, including knowledge of advanced persistent threats (APTs), malware analysis, and network forensics. However, there is a well-documented gap between the demand for skilled threat hunters and the available talent pool. This shortage not only hampers the ability of organizations to effectively implement threat hunting practices but also drives up costs, as companies must invest heavily in recruiting and retaining top talent. The growing complexity of cyber threats further exacerbates this challenge, as finding individuals with the necessary skills to combat evolving threats becomes increasingly difficult.

High Costs

Implementing effective threat hunting solutions can be prohibitively expensive, particularly for small and medium-sized enterprises (SMEs). The costs associated with advanced threat hunting platforms, tools, and managed services can be substantial. Additionally, organizations must factor in the ongoing costs of maintaining and updating these solutions to stay ahead of emerging threats. For many SMEs, these expenses can be a barrier to entry, limiting their ability to leverage advanced threat hunting technologies and leaving them vulnerable to cyberattacks. The high costs of threat hunting solutions pose a challenge for organizations looking to balance their cybersecurity budgets while ensuring adequate protection against sophisticated threats.

+44 20 8123 2220
info@marketpublishers.com

Integration with Existing Systems

Integrating threat hunting tools and platforms with existing IT infrastructure can be complex and challenging. Organizations often operate with a diverse range of systems, applications, and security solutions that may not be fully compatible with new threat hunting technologies. This can lead to issues with data integration, interoperability, and overall effectiveness of threat hunting efforts. Ensuring that threat hunting tools can seamlessly work with existing systems is crucial for effective threat detection and response. The complexity of integration can slow down the deployment of new technologies and diminish their overall impact, creating a significant challenge for organizations looking to enhance their cybersecurity posture.

Data Privacy and Compliance

Threat hunting involves collecting and analyzing large volumes of data from various sources within an organization’s network. This process raises significant concerns about data privacy and regulatory compliance. Organizations must ensure that their threat hunting activities comply with data protection regulations such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the United States. Balancing effective threat detection with the need to protect sensitive information and adhere to legal requirements is a complex challenge. Failure to address these concerns can result in legal repercussions and damage to an organization’s reputation.

Key Market Trends

Integration of AI and Machine Learning

The integration of Artificial Intelligence (AI) and Machine Learning (ML) is revolutionizing the global threat hunting market. AI and ML technologies enhance threat detection and response capabilities by automating the analysis of vast amounts of data and identifying patterns indicative of cyber threats. These technologies enable threat hunting tools to perform advanced analytics, detect anomalies, and predict potential security breaches with greater accuracy. Machine learning algorithms can continuously learn and adapt to evolving threat landscapes, improving their ability to identify sophisticated threats that traditional methods might miss. As organizations face increasingly complex and dynamic cyber threats, the adoption of AI and ML is becoming crucial for effective threat hunting.

+44 20 8123 2220
info@marketpublishers.com

Increased Adoption of Managed Threat Hunting Services

Managed threat hunting services are gaining traction as organizations seek to enhance their cybersecurity posture without the need for extensive in-house resources. These services, offered by specialized providers, deliver expert threat hunting capabilities and advanced tools on a subscription basis. Managed services are particularly appealing to small and medium-sized enterprises (SMEs) that may lack the expertise or budget to build and maintain a dedicated threat hunting team. By outsourcing threat hunting, organizations can leverage the specialized skills of external experts, access advanced technologies, and benefit from continuous monitoring and response services. This trend is driven by the increasing complexity of cyber threats and the need for cost-effective, scalable solutions.

Focus on Threat Intelligence Integration

The integration of threat intelligence with threat hunting tools is becoming a key trend in the market. Threat intelligence provides valuable contextual information about emerging threats, attack vectors, and adversary tactics. By incorporating threat intelligence into their threat hunting processes, organizations can enhance their ability to identify and mitigate threats more effectively. This integration enables threat hunters to use real-time data and insights to prioritize their efforts and respond to threats more swiftly. The growing availability of threat intelligence feeds and platforms is driving this trend, as organizations seek to stay ahead of potential threats and improve their overall security posture.

Expansion into Cloud and IoT Security

As organizations increasingly adopt cloud computing and Internet of Things (IoT) technologies, the need for specialized threat hunting solutions for these environments is rising. Cloud and IoT environments introduce new attack vectors and complexities that traditional threat hunting tools may not fully address. As a result, there is a growing demand for threat hunting solutions tailored to these environments. Cloud-based threat hunting tools are designed to protect data and applications hosted in the cloud, while IoT-focused solutions address the unique security challenges posed by connected devices. The expansion into cloud and IoT security reflects the broader trend of adapting threat hunting strategies to evolving technology landscapes.

Segmental Insights

+44 20 8123 2220
info@marketpublishers.com

Component Insights

Services segment dominated in the Global Threat Hunting market in 2023, due to several critical factors driving its growth and prominence. This dominance can be attributed to the increasing complexity of cyber threats, the need for specialized expertise, and the evolving requirements of organizations seeking to enhance their cybersecurity posture. One primary reason for the prominence of the services segment is the growing sophistication and volume of cyber threats that organizations face. Modern cyber attacks, including advanced persistent threats (APTs) and zero-day exploits, require highly specialized knowledge and advanced tools to detect and mitigate effectively. Many organizations, particularly small and medium-sized enterprises (SMEs), lack the in-house expertise and resources to address these complex threats. Managed threat hunting services provide access to seasoned cybersecurity professionals who can deliver expert analysis and threat detection capabilities without the need for substantial internal investment. These services offer not only threat hunting but also continuous monitoring, incident response, and vulnerability management, ensuring comprehensive protection against evolving threats.

The dynamic and fast-paced nature of the cybersecurity landscape demands ongoing adaptation and upskilling. Service providers in the threat hunting market are continuously updating their tools and methodologies to stay ahead of emerging threats. By outsourcing to managed services, organizations benefit from the latest technologies and practices without having to constantly update their internal systems. This is particularly advantageous in an environment where cyber threats evolve rapidly and require timely responses. Furthermore, regulatory compliance and data privacy concerns are pushing organizations to seek managed services. As data protection regulations become stricter, companies must ensure robust security measures and prompt incident response. Managed threat hunting services help organizations meet these regulatory requirements by providing expert oversight and documentation of security activities.

Regional Insights

North America dominated the Global Threat Hunting market in 2023, due to a confluence of factors that underscore the region's leadership in cybersecurity. This dominance can be attributed to the advanced technological infrastructure, high levels of investment in cybersecurity, and the presence of a robust and mature market for threat hunting solutions. One significant factor is the region’s advanced technological landscape. North America, particularly the United States, is home to a vast number of

+44 20 8123 2220
info@marketpublishers.com

leading technology companies and cybersecurity firms that drive innovation in threat hunting tools and services. The region's well-established IT infrastructure supports the deployment and integration of sophisticated threat hunting solutions, enabling organizations to stay ahead of emerging cyber threats. High levels of investment in cybersecurity further bolster North America's dominance. Both private sector companies and government agencies in the region allocate substantial resources to enhance their cybersecurity defenses. This includes funding for advanced threat detection technologies, research and development, and cybersecurity talent. The substantial financial commitment reflects the critical importance of cybersecurity in North American businesses and institutions, fostering a thriving market for threat hunting services and solutions.

North America's mature threat landscape contributes to its market dominance. The region faces a high volume of cyber threats, including advanced persistent threats (APTs), ransomware, and other sophisticated attacks. This high threat environment drives demand for proactive threat hunting to detect and respond to potential breaches before they cause significant damage. The presence of a skilled cybersecurity workforce and the availability of advanced threat hunting tools further support North America's position as a leader in the market. Regulatory and compliance requirements also play a role. North American organizations are subject to stringent data protection regulations and industry standards, which necessitate robust threat hunting capabilities to ensure compliance and safeguard sensitive information.

Key Market Players

CrowdStrike, Inc.

IBM Corporation

Palo Alto Networks, Inc.

Sumo Logic, Inc.

Elasticsearch B.V.

Broadcom, Inc.

McAfee, LLC

+44 20 8123 2220
info@marketpublishers.com

Cisco Systems, Inc.

Check Point Software Technologies Ltd.

SentinelOne, Inc.

Report Scope:

In this report, the Global Threat Hunting Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Threat Hunting Market, By Component:

Solutions

Services

Threat Hunting Market, By Deployment Mode:

On-Premises

Cloud-Based

Hybrid

Threat Hunting Market, By Organization Size:

Large Enterprises

SMEs

Threat Hunting Market, By Industry Vertical:

BFSI

Healthcare

Government

+44 20 8123 2220
info@marketpublishers.com

Retail

Manufacturing

Telecommunications

Others

Threat Hunting Market, By Threat Type:

Advanced Persistent Threats

Insider Threats

Malware

Phishing

Threat Hunting Market, By Region:

North America

United States

Canada

Mexico

Europe

Germany

France

United Kingdom

Italy

+44 20 8123 2220
info@marketpublishers.com

Spain

South America

Brazil

Argentina

Colombia

Asia-Pacific

China

India

Japan

South Korea

Australia

Middle East & Africa

Saudi Arabia

UAE

South Africa

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Threat Hunting Market.

Available Customizations:

Global Threat Hunting Market report with the given market data, TechSci Research

+44 20 8123 2220
info@marketpublishers.com

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

6. NORTH AMERICA THREAT HUNTING MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

7. EUROPE THREAT HUNTING MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

8. ASIA PACIFIC THREAT HUNTING MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

9. MIDDLE EAST & AFRICA THREAT HUNTING MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

10. SOUTH AMERICA THREAT HUNTING MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Threat Hunting Market - Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Solutions, Services), By Deployment Mode (On-Premises, Cloud-Based, Hybrid), By Organization Size (Large Enterprises, SMEs), By Industry Vertical (BFSI, Healthcare, Government, Retail, Manufacturing, Telecommunications, Others), By Threat Type (Advanced Persistent Threats, Insider Threats, Malware, Phishing), By Region and Competition, 2019-2029F

Product link: https://marketpublishers.com/r/T057213F56D3EN.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/T057213F56D3EN.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

+44 20 8123 2220
info@marketpublishers.com

& Conditions at https://marketpublishers.com/docs/terms.html

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